

27 MARCH 2003



Acquisition

PROGRAM PROTECTION PLANNING

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ USAF/XOFI (Mr. Danny Green)
Supersedes AFI 31-701, 18 Feb 94; AFI 31-702,
18 Feb 94; and AFI 31-703, 7 Feb 94

Certified by: SAF/AQX (Mr. Blaise Durante)
Pages: 67
Distribution: F

This pamphlet complements Air Force Policy Directive (AFPD) 63-17, *Technology and Acquisition Systems Security Program Protection*. It applies to Air Force, Air Force Reserve, and Air National Guard personnel engaged in Air Force technology and acquisition processes. This pamphlet addresses recommended procedures for program protection planning, systems security engineering, and other security requirements levied on contractors. Use this pamphlet with Department of Defense (DoD) Directive 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*, DoD 5200.1-M, *Acquisition Systems Protection Program*, and Air Force Instruction (AFI) 63-1201, *Assurance Of Operational Safety, Suitability, & Effectiveness*. This is a new document that consolidates some of the information previously contained in AFI 31-701, *Program Protection Planning*, AFI 31-702, *System Security Engineering*, and AFI 31-703, *Product Security*. Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule*. Any reporting requirement in this publication is exempt from licensing in accordance with AFI 33-324, paragraph 2.11.1, *The Information Collections and Reports Management Program; Controlling Internal, Public and Interagency Air Force Information Collections*.

Chapter 1—POLICY AND PROGRAM MANAGEMENT	3
1.1. Policy.	3
1.2. Philosophy.	3
1.3. Responsibilities.	5
Chapter 2—PROGRAM PROTECTION PLANNING	6
2.1. Risk Management.	6
2.2. Life-Cycle Perspective.	6
2.3. Planning Determination.	6
2.4. The System Security Working Group (SSWG).	6
2.5. Responsibilities for Program Protection Planning.	6

Table 2.1.	Program Protection Plan Criteria	7
2.6.	Coordination.	7
2.7.	The Program Protection Plan (PPP).	7
Table 2.2.	Requesting a Threat Assessment.	10
2.8.	The Technology Protection Plan (TPP).	20
2.9.	Operational Command Protection Planning Requirements.	20
Chapter 3—	SYSTEMS SECURITY ENGINEERING (SSE)	22
3.1.	Purpose.	22
3.2.	Vulnerabilities.	22
3.3.	Procedures.	22
3.4.	Operational and Support MAJCOMs, Field Operating Agencies, and Supporting Security Forces Requirements	22
3.5.	SSE Approach.	23
3.6.	SSE Process Tool.	23
Chapter 4—	SECURITY MANAGEMENT	24
4.1.	General.	24
4.2.	Contractual Requirements for the Protection of Classified Information.	24
4.3.	Additional Security Requirements.	24
Table 4.1.	List of Additional Security Considerations (NOTE 1).	27
Chapter 5—	PROGRAM PROTECTION SURVEYS (PPS)	29
5.1.	General.	29
5.2.	PPS Objectives.	29
5.3.	Purpose.	29
5.4.	Information Collections, Records, and Forms.	30

AFPAM63-1701 27 MARCH 2003	3
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	31
Attachment 2—MEMORANDUM FROM THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS, RESEARCH AND TECHNOLOGY - PROTECTION PROGRAM PLANS, 30 JUNE 2000	37
Attachment 3—THE SYSTEM SECURITY WORKING GROUP (SSWG)	39
Attachment 4—SECURITY WORK BREAKDOWN STRUCTURE (WBS)	42
Attachment 5—SYSTEM SECURITY ENGINEERING PROCESS TOOL	46

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.1. Policy. It is DoD policy that security is an equal partner in systems acquisition to schedule, cost, performance, and supportability. See [Attachment 2](#).

1.2. Philosophy. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* defines security as: “1. Measures taken by a military unit, an activity, or installation to protect itself against all acts designed to, or which may impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3. The condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.” Security can be thought of as an end-state that emphasizes protection and prevention through established measures that strive to achieve a condition free from hostile acts/influences. It is a proactive, results-oriented system of integrated activities, programs, facilities, and policies designed to preserve Air Force people, information, facilities, property, and equipment in order to enable aerospace capability.

1.2.1. The objective of program protection planning is to protect critical information, technology and resources associated with acquisition systems to insure the Air Force can acquire, field and operate quality weapon and support systems, that have not been compromised, to meet mission requirements. The program is designed to:

1.2.1.1. Identify science and technology (S&T), or program information, technologies, processes, applications, or end items that, if compromised, would: degrade system combat effectiveness of existing or future systems; compromise the program or system capabilities; allow reverse-engineering of critical system capabilities; shorten the expected combat-effective life of the system; significantly alter program direction; or, require additional resources to counter the impact.

1.2.1.2. Identify critical information, technology, infrastructures, and systems that, if denied, degraded, or destroyed, would significantly impact the warfighters ability to meet mission requirements.

1.2.1.3. Identify fundamental security requirements that must be met in order to certify and operate the system.

1.2.1.4. Assess collection capabilities of foreign interests.

1.2.1.5. Identify potential threats.

1.2.1.6. Identify security vulnerabilities.

1.2.1.7. Determine cost-effective security measures using risk management analyses to eliminate or mitigate security vulnerabilities and comply with designated security requirements.

1.2.1.8. With the recommendations from the System Security Working Group (SSWG), develop and implement the Technology Director (TD) approved time-phased or event driven security measures into the appropriate technology plan or Program Manager (PM) approved time-phased or event-driven security measures into the integrated master plan, integrated master schedule and life cycle cost model, carefully considering and periodically assessing acceptable risk.

1.2.2. Program protection planning is an effects-based program. It encompasses the evaluation and integration of multiple security, intelligence, and counterintelligence processes that should be tailored into and throughout the Research, Development, Test and Evaluation (RDT&E), acquisition, Operational Test and Evaluation (OT&E), operational, and sustainment phases of a system using sound risk management analyses. Some of these processes outline requirements that should be integrated into acquisition documentation, engineering documentation, test plans, technical orders, and facility/resource requirements documents levied by the acquisition community on the user. The TD or PM should assign the Chief Engineer or Scientist to chair the system security working group to comprehensively evaluate all security, intelligence, and counterintelligence inputs as the working group develops recommended requirements (i.e., physical security, Communications Security (COMSEC), Computer Security (COMPUSEC), Operations Security (OPSEC), infrastructure assurance), and integrate those requirements into existing technology, system and program documentation.

1.2.3. Air Force program protection planning is a life-cycle program, providing protection from cradle to grave. In order to meet objectives, the program should begin in the earliest phases of acquisition. The Program Manager, as the initial resource manager, and the Milestone Decision Authority, as the approval authority, are ultimately responsible for acquiring a system that effectively prevents compromise and is inherently securable so that it can accomplish its mission in a hostile environment. However, equally critical to the success of the program is the active participation of the operational commander who will become the resource manager when the system is delivered to the operational command. Inclusion of the resource manager on the SSWG would provide the scientists, engineers, and team members with valuable insight into the operational requirements needed to assist the resource manager in making informed protection decisions and consciously managing risk.

1.2.4. In rare cases, the need for system program protection may occur before formal systems acquisition. Basic research is, of necessity, conducted in an inherently open environment to maximize the opportunity for productive advancement and minimize the possibility of pursuing concepts that another agency has already proved to be fruitless. The transition from basic research to applied research to advanced technology development then to system development is normally not a defined event. TDs should be vigilant in monitoring their programs and, when breakthrough research, technology, or systems emerge, the guidance of this pamphlet may be tailored to provide protection until the research transitions into an acquisition program.

1.2.5. The Air Force program protection planning process is a critical tool for the Air Force to develop, acquire, and field secure and uncompromised weapon systems. The program identifies and protects both classified and unclassified critical program information (CPI) and critical system resources (CSR) for each defense acquisition program. Program protection planning from the Concept and Technology Development phase (Milestone A), through all phases of the development and acquisition process, to system demilitarization should be accomplished as outlined in this pamphlet.

1.2.6. This pamphlet integrates all security, intelligence, and counterintelligence disciplines into a cross-functional team approach that concentrates on risk identification, analysis, and management. Program protection planning provides TDs, PMs, system owners, system operators, and system supporters with a comprehensive approach to assess threat data and identify countermeasures they can use to evaluate the risk and eliminate or mitigate threats.

1.2.7. Program protection planning provides a basis for balancing risks, security countermeasures, and security costs to the system being procured.

1.3. Responsibilities.

1.3.1. PMs determine Program Protection Plan (PPP) requirements IAW AFPD 63-17 when information, technologies, and/or systems are deemed to require protection.

1.3.2. TDs determine Technology Protection Plan (TPP) requirements IAW AFPD 63-17 when information or technologies are deemed to require protection.

1.3.3. Owning, operating, and supporting Major Commands (MAJCOM) and agency commanders (from this point forward referred to as "using commands") should participate in the modernization planning process; Mission Needs Statement (MNS) development and updates; Operational Requirement Documents (ORD) development and updates; identifying thresholds and objectives for system security engineering, anti-tamper and technology/program protection requirements; Program Management Directive (PMD) development and updates; and other protection documentation to ensure deployment, operational, and support protection issues are sufficiently addressed.

1.3.4. The Milestone Decision Authority (MDA), Air Force Program Executive Officer, or Designated Acquisition Commander, as appropriate, is responsible for reviewing and validating the program protection requirements identified by the PM as well as the measures proposed to satisfy these requirements.

1.3.5. Information Security Program Managers (ISPM), as defined in AFI 31-401, at all levels, should provide security guidance and assistance to TDs and PMs as necessary. This may include, but is not limited to, conducting surveys, participating on security working groups, reviewing documents/plans (e.g., TPP, PPP, MNS, and ORD) and technical assistance in developing security classification guidance.

Chapter 2

PROGRAM PROTECTION PLANNING

2.1. Risk Management. Preparation and implementation of a PPP relies on operational risk management (ORM), not risk avoidance. TDs/PMs must balance the level and cost of protecting critical resources or information against the cost and impact to the program as a whole.

2.2. Life-Cycle Perspective. The PPP integrates and guides management of system security for an acquisition program throughout its life-cycle to include demilitarization.

2.3. Planning Determination. PMs will determine the existence of CPI/CSR within their program areas IAW AFPD 63-17. This examination should also consider protection requirements previously identified by DoD laboratories, as well as CPI and CSR inherited from another program, or as a result of non-traditional acquisition techniques (e.g., Advanced Concept Technology Demonstration, flexible technology insertion, etc.) and the need to identify protection requirements for government owned and private infrastructures necessary for mission accomplishment. A methodology to identify CPI/CSR may be found in paragraph 2.7.2.3. of this pamphlet. Air Force acquisition programs with identified CPI/CSR will have a PPP.

2.3.1. The PPP must be approved by the Milestone Decision Authority (MDA), or their designee IAW AFPD 63-17. Approval of the PPP will not be delegated below the PM.

2.3.2. If the PM determines that there is no CPI or CSR associated with the program (neither integral to the program nor inherited from a supporting program), a PPP is not required. The PM should make this determination in writing for review by the MDA.

2.3.3. The PM will, in coordination with SAF/AAZ, determine the need for a PPP when special access program information is involved, IAW AFPD 63-17.

2.3.4. If Sensitive Compartmented Information (SCI) will be used in association with a system, coordinate the PPP with the cognizant Special Security Office (SSO) IAW AFPD 63-17.

2.3.5. Regardless of where the program is in the acquisition process, a PPP should be developed as soon as CPI or CSR is identified.

2.4. The System Security Working Group (SSWG). When CPI/CSR is present, PMs should establish a SSWG to assist in the planning process. See Attachment 3 for further details.

2.5. Responsibilities for Program Protection Planning.

2.5.1. The PM has ultimate responsibility for the PPP, although using commands will be involved in the planning process as part of the management and milestone reviews. See paragraph 2.7. and Attachment 3 of this pamphlet.

2.5.2. PMs should designate a senior scientist or chief engineer to insure all program protection planning activities are coordinated through the SSWG. The PM should insure the PPP is used as a life cycle planning and programming document. The PPP should be reviewed during each budget planning cycle.

2.5.3. Table 2.1. provides criteria for an effective PPP.

Table 2.1. Program Protection Plan Criteria

1. Does the summary of the system description identify the system's mission, military value, and expected operational parameters?
2. Does the description of the CPI/CSR identify the significant technical parameters, which, if compromised, would reduce the combat effectiveness or combat effective lifetime of the system?
3. Does the threat and or vulnerability analysis: <ul style="list-style-type: none"> a. Identify who has the interest and capability to collect information about the system or damage, degrade, or destroy it? b. Indicate which other countries are performing research in these areas, what is the level of sophistication, and how well they are protecting or controlling the information?
4. Does the countermeasures program: <ul style="list-style-type: none"> a. Indicate that it is time or event driven in its implementation or termination of protection strategies? b. Commit to a level of protection or security concept that will assure a minimal level of protection for the essential elements?
5. Does the cost criteria provide the data by acquisition phase?

2.6. Coordination. PPP development and implementation requires close coordination between the PM, key members of the program office, user commands, and the security, Counterintelligence (CI), and intelligence communities.

2.7. The Program Protection Plan (PPP).

2.7.1. The PPP is the single-source document to coordinate and integrate protection efforts. The PPP identifies elements of the program, classified and unclassified, which require protection to prevent unauthorized disclosure, or inadvertent transfer of critical technology or information. Development of the PPP begins upon initial identification of CPI/CSR. It should be updated as required. The PPP should be reviewed by the MDA at the first review after the identification of CPI/CSR.

2.7.2. The following elements should be included in all PPPs. Note that these are recommended minimum requirements, but the PM may tailor its composition as necessary. The PPP is a "living document" and should be updated as necessary.

2.7.2.1. System Description. The system description should clearly indicate capabilities and limitations of the system, including support equipment and simulators. It should include:

2.7.2.1.1. The anticipated battlefield employment of the system.

2.7.2.1.2. The strategic, operational, or tactical impact of the system's development and deployment.

2.7.2.1.3. The specific characteristics that distinguish it from existing systems or other systems under development.

2.7.2.1.4. The function, operational characteristics, and technical parameters of any component program, product, technology demonstrator, or other acquisition system that is an integral part of the system.

2.7.2.2. Program Information. Program information details the organization and structure of the office responsible for developing and fielding the acquisition system. Use the program information to briefly describe the chain of command for the program, including the program's decision authority and any sub-programs, and specify the location, points of contact, and telephone numbers of the following:

2.7.2.2.1. Government-owned sites that will handle CPI/CSR material.

2.7.2.2.2. Government-owned test and evaluation centers where CPI/CSR material will be tested.

2.7.2.2.3. Primary contractors who handle CPI/CSR materials.

2.7.2.2.4. Contractor-owned facilities where CPI/CSR materials will be designed, developed, processed, tested, stored, produced, supported, and managed.

2.7.2.3. List of CPI and CSR. The CPI and CSR are the critical elements of the system that make it unique and valuable to U.S. forces, and if compromised, would cause a degradation of combat effectiveness, decrease the combat-effective life-cycle, or allow a foreign activity to clone, kill, or neutralize the system. It is these pieces of technology, hardware, or information that must be protected.

2.7.2.3.1. CPI and CSR can include components, engineering, design or manufacturing processes, and technologies; system capabilities and vulnerabilities; and other information that gives the system its unique battlefield capability or limits the ability of other countries to reproduce the essential capability or mission.

2.7.2.3.2. The first step in identifying CPI and CSR is for the PM (or representative) and the chief scientist or chief systems engineer to facilitate functional decomposition or "breakdown" of the system. Scientists, security professionals, OPSEC managers, and CI/intelligence personnel may be used to assist in this process.

2.7.2.3.2.1. Beginning with the system description, identify those specific components or attributes that give the system its unique ability.

2.7.2.3.2.2. Similarly, analyze each subsystem and subassembly until specific technology, equipment, or processes are identified.

2.7.2.3.2.3. Once the technology, equipment, or processes are identified, the PM will evaluate their potential as CPI and CSR by applying the following questions. An affirmative answer to any of these questions qualifies an item as CPI or CSR.

2.7.2.3.2.3.1. Could loss or compromise result in destruction of the system?

2.7.2.3.2.3.2. Could loss or compromise result in degradation or neutralization of the system?

2.7.2.3.2.3.3. Could loss or compromise result in duplication of the system?

2.7.2.3.2.3.4. Could loss or compromise degrade system combat effectiveness; compromise the program or system capabilities; shorten the expected combat-effective life of the system; significantly alter program direction; or, require additional resources?

2.7.2.3.2.3.5. Could loss or compromise adversely impact other existing capabilities, degrading the Air Force's ability to carry out its mission?

2.7.2.3.3. The PM should prioritize the CPI/CSR list for use during threat/vulnerability assessments, program protection planning, and analysis of the protection costs. Criteria listed in paragraph 2.7.2.5.2. may be used for this purpose.

2.7.2.4. Threats to CPI and CSR.

2.7.2.4.1. The AFOSI Research and Technology Protection (RTP) program provides CI support to RDT&E facilities, acquisition programs, personnel, and existing or restricted technologies. Through these efforts, the RTP specialist will work closely with the PM for monitoring and tracking supported CPI/CSR and technologies identified by the PM during the life-cycle process. The specific CI RTP requirements should be documented in the CI Support Plan (CISP). A CISP is an agreement with the customer (PM) and the supporting AFOSI used to integrate CI into the overall security effort. The CISP should be included in the PPP. It is a living document that is modified as the technology and/or program, or its CPI/CSR transition. The CISP should be revalidated as necessary to ensure currency and relevancy.

2.7.2.4.1.1. When CPI or CSR is present, PMs should request a counterintelligence threat assessment from their servicing RTP specialist, and an intelligence assessment from the servicing intelligence organization. A list of questions is provided in Table 2.2. as a guide to prepare the request.

Table 2.2. Requesting a Threat Assessment.

1. Name of Program/Project/Product.
2. Program/Project/Product Manager, Organization, Location, and Telephone Numbers.
3. Security Manager Address and Telephone Numbers.
4. Contract Numbers/Prime Contractor/Location/Mailing Address/Security Manager/Telephone number.
5. Major Subcontractors/Address/Subcontract numbers/Security Managers/Telephone Numbers.
6. Against what will the system be targeted?
7. What are the program's CPI and CSR?
8. What specific technologies do you need to protect? Which contractor(s) is involved?
9. What specific information of core technologies is classified? Is special access program technology involved?
10. Where are the technologies located (e.g., aboard aircraft, within buildings, mounted in vehicles, man-packed, etc.)?
11. If the material is a weapons system, what specific component or components require protection (e.g., sights, range finder, target acquisition system, is the system or technology touch or sight sensitive, etc.)?
12. If you are protecting a computer system, what specific component(s) of the system requires protection (e.g., software, hardware, etc.)?
a. Is the system stand-alone or networked?
b. Can you access the system from other systems at other facilities or bases?
c. Are links between systems encrypted?
d. How are the systems linked (e.g., dedicated land lines, microwave, etc.)?
13. If an aircraft is involved, what specific component of the aircraft requires protection (e.g., electronic system, weapon system, crew, etc.)?
a. Can you remove the components from the aircraft?
b. Can you see the components from outside the aircraft?
14. If vehicles are involved, are the vehicles dedicated to this system or activity?
a. Are these vehicles unique to this system or activity?
b. Can you see the system components from outside the vehicle?
c. Can you remove the components of the system from the vehicle?

15. What are the identifiable, exploitable characteristics of the technology?
a. Are there unique physical characteristics involved?
b. Can you see the characteristics of the system from outside it?
c. Does the system have an electronic signal emission?
d. What is the system's operating frequency range?
e. Is the system active or passive?
f. What is the system's power output?
g. What is the system's range?
16. Are there specific communications associated with this system?
a. Where are these systems employed? (Indicate the location of bases or facilities.)
b. How will you use the system?
17. With what facilities is the system associated?
a. Are the facilities unique to the system?
b. Can you see the facilities from the outside?
c. Where are the facilities located (e.g., military base, civilian community, industrial complex, public building, etc.)?
d. What access controls exist for the building?
18. What aspects of the training must you protect? (Indicate particular activities, participants, location, association with system, etc.)
19. Where will you do the system testing? (Indicate any previous test dates, locations, as well as future test dates and locations.)
20. Is the system site sensitive (that is, are you worried about the site being seen)? If yes, why?
21. What types of emissions to systems tests or test sensors generate?
22. Has or will any testing be done against actual or simulated foreign equipment? If yes, identify the foreign equipment, test locations, and dates.
23. Do any plans exist, or have there been inquiries about, foreign involvement (e.g., foreign sales, foreign cooperative development, co-production, joint ventures, etc.)? If yes, with whom are negotiations taking place and what is the current status?
24. What are the major milestone dates for this program?
(NOTE: Use derivative or Original Classification Authority determination to classify this request as necessary.)

2.7.2.4.1.2. The servicing RTP specialist and the servicing intelligence organization should analyze the full spectrum of threats against the CPI or CSR, providing a complete and detailed report to the PM.

2.7.2.4.1.3. Upon receipt of the threat assessment from intelligence and/or counterintelligence, the PM should forward the report to the SSWG for action. SSWG actions include,

but are not limited to: the evaluations of all security, intelligence, and counterintelligence requirements, the assessment of threat data, conducting risk analysis, conducting vulnerability assessments, evaluating and recommending new or additional countermeasures, identifying countermeasure cost estimates, recommending updates to the PPP and annexes and providing system security and technology protection inputs into the acquisition strategy, program schedules and plans, security classification(s), a plan to mitigate potential threats, including those that could arise from verification provisions of nonproliferation and other treaties, agreements or regimes, etc.

2.7.2.4.1.4. Servicing intelligence organizations should provide information on technical capabilities of adversaries in specific RDT&E programs or projects.

2.7.2.4.1.5. Working together, RDT&E, CI, security, foreign disclosure, OPSEC, and intelligence organizations should use an interactive process to safeguard CPI and CSR from compromise in order to sustain or advance the technological lead in the current and future battlespace.

2.7.2.4.1.6. PMs, in coordination with intelligence, and CI specialists, should ensure that assigned personnel receive tailored threat briefings.

2.7.2.4.1.7. PMs should prepare, using SSWG resources as appropriate, a comprehensive plan to mitigate any potential threat to USAF/DoD facilities that could be subjected to on-site verification activities resulting from nonproliferation and other treaties, agreements, or regimes (e.g., Chemical Weapons Convention, START, Open Skies, etc.).

2.7.2.4.2. Foreign Collection Threat

2.7.2.4.2.1. Foreign collection threat assessments used by the program office in planning protection for the CPI and CSR should be based upon a National-level intelligence estimate.

2.7.2.4.2.1.1. The National-level threat assessment should be prepared and produced as a stand-alone document.

2.7.2.4.2.1.2. The National-level analysis should identify foreign interests having a collection requirement and capability to gather information about the system being developed.

2.7.2.4.2.1.3. Sudden changes in the operational threat should be reviewed as they occur to determine if the changes are due to successful foreign intelligence collection.

2.7.2.4.2.1.4. The PM and SSWG should compare results of the National-level threat assessment with the CPI/CSR to determine vulnerabilities and the level of risk to the program.

2.7.2.4.2.1.5. The SSWG should integrate environmental factors and arms control-related issues that might reduce the ability of foreign interests to collect information at a given location in the National-level threat assessment, where applicable.

2.7.2.4.2.2. A threat exists when:

2.7.2.4.2.2.1. A foreign interest has a confirmed or assessed requirement for acquiring program information; and/or

2.7.2.4.2.2.2. a foreign interest has the capability to acquire such information.

2.7.2.4.2.3. Confirmed or assessed identification of foreign collection requirements provides indications of probable sources and methods that might be employed to satisfy a collection requirement.

2.7.2.5. Vulnerability of CPI and CSR to the Threats. Vulnerabilities are the susceptibility of the program to the threat(s) in a given environment. In other words:

SUSCEPTIBILITY + THREAT = VULNERABILITY

2.7.2.5.1. The vulnerabilities possessed by the program's CPI/CSR should be based upon the ability of a threat source to collect directly on the CPI, or information indicative of it, or damage, degrade or destroy CSR. Some factors to be considered are:

2.7.2.5.1.1. How the CPI and CSR are stored, maintained, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, or modem).

2.7.2.5.1.2. How the CPI and CSR are used (e.g., bench testing or field testing).

2.7.2.5.1.3. What emanations, exploitable signals, or signatures are generated by the CPI and CSR or reveal them (e.g., telemetry, acoustic, or radiant energy).

2.7.2.5.1.4. Where the CPI and CSR are located (e.g., program office, test site, contractor, or vendor).

2.7.2.5.1.5. What types of OPSEC indicators or observables are generated by program or system functions, actions, and operations involving CPI and CSR.

2.7.2.5.2. Once the vulnerabilities are identified, the PM should place them in priority sequence order.

2.7.2.5.2.1. The sequence should be based upon the consequences of the loss or compromise of the CPI and CSR that are involved.

2.7.2.5.2.2. Factors that should be considered include the impact upon the combat effectiveness of the system, the effect on the combat-effective lifetime of the system, the cost associated with any modification required to compensate for the loss, and the choice of alternatives (such as the technology used or the test range used) that are available.

2.7.2.6. Security Classification Guide (SCG). A time or event phased SCG should be developed and maintained for each acquisition program, as necessary. Use DoD 5200.1-H, *Department of Defense Handbook for Writing Security Classification Guidance*, in preparing the SCG.

2.7.2.6.1. Prepare the SCG after identifying the system's classified CPI and CSR. For acquisition programs, an original classification authority should approve the guide no later than Milestone B. The SCG should be updated as necessary.

2.7.2.6.2. The completed SCG should be attached to the PPP.

2.7.2.6.3. Focus on the CPI and CSR. Consider whether unclassified CPI and CSR should be marked with distribution statements or other protection requirements.

2.7.2.7. Technology Assessment/Control Plan.

2.7.2.7.1. A Technology Assessment/Control Plan (TA/CP) must be approved for all acquisition programs that will have foreign military sales IAW AFPD 63-17. The TA/CP should be completed before submitting the request for authority to negotiate an international agreement. Coordinate the TA/CP with the appropriate local offices to get approval for foreign disclosure, foreign cooperation or co-production, and foreign military sales (if applicable).

2.7.2.7.2. The TA/CP serves three purposes:

2.7.2.7.2.1. Assesses the feasibility of U.S. participation in joint programs from a foreign disclosure and technical security perspective.

2.7.2.7.2.2. Supports drafting of the Delegation of Disclosure Authority Letter (DDL). A DDL is a prerequisite to the disclosure of U.S. Government information to foreign entities.

2.7.2.7.2.3. Serves as a supporting document during acquisition decision review.

2.7.2.7.3. Content. The TA/CP consists of two sections:

2.7.2.7.3.1. The Technology Assessment Section. This section focuses on the risk to the U.S. of disclosing technology or information to other countries. Identify the technology of concern, its classification or control method, and why it is under development. Evaluate the availability of comparable foreign technology, previously released U.S. technologies, and any material released under other programs. Finally, compare the value in terms of technologies and military capabilities, and possible damage resulting from compromise of these technologies or capabilities.

2.7.2.7.3.2. The Control Plan Section. This section describes the measures necessary to minimize potential risk associated with the material's release. Discuss phasing the release of information to reduce the risk of compromise using disclosure restrictions and using special security procedures to limit access to critical information. Include a discussion of any modification to the system, design, or production produced under the agreement, or any legal or proprietary concerns associated with such an agreement.

2.7.2.7.3.3. In addition, the program office prepares a DDL as part of the request for authority to conclude an agreement. Reference AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*, for further guidance for preparation and coordination of DDLs.

2.7.2.8. System Security Engineering Considerations (Risk Mitigation).

2.7.2.8.1. System security engineering applies scientific and engineering principles to identify system vulnerabilities and eliminate or contain associated risks. System security engineering is an essential element of acquisition systems protection and integrates security into the overall systems engineering process.

2.7.2.8.2. System security engineering seeks to eliminate, reduce, or control through engineering and design, any characteristics that could allow deployment of systems with operational security deficiencies. For more detailed information on system security engineering, refer to [Chapter 3](#) of this pamphlet.

2.7.2.9. Countermeasures.

2.7.2.9.1. Countermeasures eliminate or reduce the projected vulnerabilities of each CPI/CSR, and, within the parameters of risk management principles, negate an adversary's ability to exploit a vulnerability.

2.7.2.9.1.1. Countermeasures should only be developed to eliminate vulnerabilities associated with an identified threat to the CPI/CSR based upon the threat analysis.

2.7.2.9.1.1.1. Countermeasures should be time or event phased.

2.7.2.9.1.1.2. Countermeasures should not be implemented until they are required, and they should be terminated or reduced as soon as possible after the threat, CPI/CSR, or environmental changes lead to a reduction or elimination of the vulnerabilities or negation of the threat.

2.7.2.9.1.2. PMs should establish countermeasures based upon a cost-benefit analysis.

2.7.2.9.1.2.1. The analysis should focus on the cost associated with the deployment of the countermeasure compared to the risk associated with loss or compromise of the essential information.

2.7.2.9.1.2.2. The cost-benefit analysis is for internal use only, and need not be an enclosure, annex, or chapter of the PPP.

2.7.2.9.1.2.3. Should countermeasures not be developed for identified CPI/CSR vulnerabilities the PM should justify this in the countermeasures section of the PPP.

2.7.2.9.1.3. Should the acquisition program not have an assigned or contracted security apparatus, the SSWG (or a similar group for technology programs) should help draft countermeasures based upon the PM's guidance and intent.

2.7.2.9.1.4. The establishment of a protection baseline is the goal of the countermeasures section of the PPP.

2.7.2.9.1.4.1. There should be a clear commitment to a level of protection to ensure protection of the CPI/CSR.

2.7.2.9.1.4.2. The minimum level of effort and cost should be applied to guarantee a level of protection appropriate to the PM's final estimate of the intelligence collection threat to the system.

2.7.2.9.1.5. Although there is not a required format for the presentation of the countermeasures section, PMs should consider the following questions when developing countermeasures:

2.7.2.9.1.5.1. Why were these specific countermeasures selected?

2.7.2.9.1.5.2. Which specific vulnerabilities do they remedy?"

2.7.2.9.1.5.3. When and how will they be implemented or increased?

2.7.2.9.1.5.4. When and how will they be terminated or reduced?

2.7.2.9.1.5.5. How much are they expected to cost?

2.7.2.9.1.5.6. Are there differences in protection levels between facilities owned by the government and by contractors, especially with regard to test facilities and the rea-

sons for the difference? (NOTE: Compliance with the PPP should be included in the list of Terms and Certifications and the Statement of Objective (SOO) of the government's solicitation.)

2.7.2.9.1.5.7. How much additional manpower will be required?

2.7.2.9.1.6. Training in technology/acquisition system protection and security awareness are integral parts of the countermeasures effort.

2.7.2.9.1.6.1. Following the approval of the PPP, PMs should implement a training program to inform all members of their program of the efforts, procedures, and methods to be used to protect CPI/CSR.

2.7.2.9.1.6.2. Strong emphasis should be placed on the encrypted transmission of electronic messages and e-mails, facsimile transmissions, and telephone transmissions relating to CPI/CSR or other unclassified technical information.

2.7.2.9.1.7. Countermeasures are dynamic and change with the passage of time. As the threat, CPI/CSR, or environment change, the countermeasures should also change. PMs should update their PPP as necessary to minimize the cost and administrative burden.

2.7.2.10. Anti-tamper Plan.

2.7.2.10.1. The PM should consider anti-tamper (AT) measures for use on any system with CPI/CSR, developed with allied partners, likely to be sold or provided to U.S. allies and friendly foreign governments, or likely to fall into enemy hands. The PM should document the analysis and recommendation to use or not to use anti-tamper measures in a classified annex to the program protection plan, and report findings to the MDA at Milestone A and subsequent milestones. The MDA should consider for approval, the PM's recommendation to implement or not to implement anti-tamper measures.

2.7.2.10.2. The Milestone A anti-tamper annex to the PPP should include the following:

2.7.2.10.2.1. A list of critical technologies.

2.7.2.10.2.2. A threat analysis.

2.7.2.10.2.3. Identified vulnerabilities.

2.7.2.10.2.4. A preliminary anti-tamper requirement.

2.7.2.10.2.5. An anti-tamper security classification guide. To determine the classification measures associated with the program, contact SAF/AQLS, DSN 425-1465, commercial 703-588-1465.

2.7.2.10.3. At Milestone B, the PM should address how anti-tamper measures will be tested during developmental testing and operational testing, and made ready for production.

2.7.2.10.4. The anti-tamper annex to the program protection plan at Milestone B should include the following:

2.7.2.10.4.1. All deliverables from Milestone A and applicable updates.

2.7.2.10.4.2. An analysis of anti-tamper methods that apply to the system, including cost/benefit assessments.

- 2.7.2.10.4.3. An explanation of which anti-tamper method(s) will be implemented.
- 2.7.2.10.4.4. Planning for validation and testing of the anti-tamper implementation. Supportability and training requirements to maintain the integrity of the anti-tamper feature(s).
- 2.7.2.10.5. The anti-tamper annex to the PPP at Milestone C should include the following:
 - 2.7.2.10.5.1. All deliverables from Milestone B and applicable updates.
 - 2.7.2.10.5.2. Anti-Tamper Validation Plan for MDA review.
 - 2.7.2.10.5.3. Anti-tamper measures demonstrated during developmental test.
 - 2.7.2.10.5.4. Anti-tamper measures ready for production.
- 2.7.2.10.6. Developmental test and evaluation should verify implementation of anti-tamper measures. During initial system production, the Air Force anti-tamper executive agent should validate anti-tamper measures on actual or representative system components provided by the PM. The anti-tamper executive agent should report validation results to the appropriate system acquisition executive and USD(AT&L) at the Full-Rate Production decision review.
- 2.7.2.10.7. Anti-tamper measures should apply throughout the life-cycle of the system. To protect critical technologies, it may be necessary to limit the level and extent of maintenance a foreign customer may perform. This will mean that maintenance involving the anti-tamper measures will be accomplished only at the contractor or U.S. Government facility in the U.S. or overseas. Such maintenance restrictions should be no different than those imposed on U.S. Government users of anti-tamper protected systems. Contracts, purchase agreements, memoranda of understanding, memoranda of agreement, letters of agreement, or other similar documents shall indicate *“The United States Government may require anti-tamper (AT) protection measures. The AT protection will not impact operations, maintenance, or logistics provided that all terms delineated in the system technical documentation are followed.”* When a contract that includes anti-tamper protection requirements and associated maintenance and logistics restrictions also contains a warranty or other form of performance guarantee, the contract terms and conditions shall establish that unauthorized maintenance or other unauthorized activities:
 - 2.7.2.10.7.1. Shall be regarded as hostile attempts to exploit or reverse engineer the weapon system or the anti-tamper measure itself; and
 - 2.7.2.10.7.2. shall void the warranty or performance guarantee.
- 2.7.2.11. Test Protection Planning. PMs, in concert with the user and test communities, identify protection requirements for Developmental Test and Evaluation (DT&E), OT&E, and other test activities. The T&E strategy should provide information about risk and risk mitigation, and determine whether systems are operationally effective, suitable and survivable against the identified threats.
- 2.7.2.12. Life-cycle Protection Costs. Direct protection costs should be detailed for each acquisition phase. Examples of protection costs include manpower, equipment, services and all other costs that directly contribute to the protection of the program. Cost estimates should be coordinated with the program control office, as follows:

2.7.2.12.1. Include in manpower costs all personnel who provide direct support to the program protection effort. Your local manpower office can guide you in determining manpower cost.

2.7.2.12.2. List equipment used in the protection effort with the associated cost. For example, include the cost of safes, secure computers, software, entry controls, alarms, construction of vault areas, administrative equipment, and security equipment engineered into the weapon system.

2.7.2.12.3. Identify miscellaneous costs not included in the previous paragraphs. Include temporary duty to support program protection, cost of transporting classified components, security education and training efforts, and contract administrative support. Prepare program protection cost estimates for the current and remaining acquisition phases for programs that have advanced beyond Milestone A. If necessary, use historical cost data as a basis for future estimates.

2.7.2.12.4. A Sample Security Work Breakdown Structure is provided at [Attachment 4](#).

2.7.2.13. Disclosure Considerations.

2.7.2.13.1. Freedom of Information Act (FOIA). PMs should evaluate and include prudent and necessary life-cycle planning to address FOIA requests IAW DoD Regulation 5400.7/Air Force Supplement 1, *DoD Freedom of Information Act Program*. The primary objective is to develop policies and methods to effectively balance public release and, when necessary, withholding of program information.

2.7.2.13.2. Withholding Of Unclassified Technical Data From Public Disclosure. PMs should evaluate and include prudent and necessary life-cycle planning to address withholding of unclassified technical data from public disclosure in accordance with DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure* and AFI 62-104, *Disseminating Scientific and Technical Information*. The primary objective is to develop policies and methods to effectively identify and withhold, when necessary, technical program data.

2.7.2.14. Foreign Disclosure. Foreign disclosure is an integral part of the TA/CP (see paragraph [2.7.2.7](#) of this instruction), and should be addressed therein.

2.7.2.15. Foreign Sales and Co-Production. Foreign Sales, Co-Production, and other potential opportunities for foreign access (e.g., during deployments outside the continental U.S. or involvement of foreign exchange officers) are an integral part of the TA/CP (see paragraph [2.7.2.7](#) of this instruction), and should be addressed therein.

2.7.2.16. Follow-On Support and Modification Management.

2.7.2.16.1. Follow-on support, as it pertains to foreign military sales, is that support provided on a day-to-day basis subsequent to the initial support period and prior to removal of the end item from the inventory. A follow-on support analysis should be conducted and documented, normally as part of the foreign sales portion of the TA/CP, to ensure all program protection planning considerations have been addressed.

2.7.2.16.2. Modification management should include all relevant aspects of program protection planning to safeguard CPI/CSR, SSE to ensure cost effective security measures are

included in the modification, and any other security requirements levied on the contractor for the modification.

2.7.2.17. Demilitarization. PMs should plan to minimize Air Force liability due to information and technology security issues as a part of demilitarization requirements.

2.7.2.18. C4I Certification and Accreditation. PMs should describe the security support required from the C4I infrastructure. Identify the information security classification level(s) required and capabilities employed. For example, if data is encrypted, describe the type of encryption planned. Address information assurance, infrastructure assurance, and protection of critical systems and infrastructures, giving special consideration to vulnerabilities resulting from reliance on other Government or civil sector infrastructures and the risk of their loss, damage, or destruction.

2.7.2.19. OPSEC Plan. PMs should use AFI 10-1101, *Operations Security (OPSEC)*, Attachment 7, to develop this portion of the PPP.

2.7.2.20. Systems Security Engineering Approach. The Systems Engineering Management Plan and the System Security Management Plan may be used to document this.

2.7.3. The sample work sheet in [Table 2.2](#) may be used to gather information to prepare the PPP. The worksheet is not a boiler-plate, "fill-in-the-blank" program protection plan. Use it to gather data for PPP planning, development, and updates. Evaluate the plan's security classification requirements by considering the scope and focus of the PPP.

2.7.4. Additional Security Plans. Attach additional security plans, as needed, as tabs to the PPP (e.g., TEMPEST Plan, Computer Systems Security Accreditation Checklist, Sensitive Compartmented Information Facility Accreditation Plan, System Security Management Plan, Weapon System Security Standard). For ease of use and storage, it is highly recommended that security classification markings for each plan be done as a stand-alone document.

2.8. The Technology Protection Plan (TPP).

2.8.1. A TPP integrates and guides management of risk to S&T programs that are focused on basic research, applied research, and advanced technology development to produce generic, not system-specific, technologies. When technologies are integrated into an acquisition program, the TPP will transfer with the technology providing the basis for the PPP.

2.8.2. TPPs should be organized like a PPP. They will address many of the same topics; however, because these plans are oriented to S&T and not a life-cycle acquisition process, they should be tailored accordingly. The TPP is a "living document" and should be updated as necessary.

2.9. Operational Command Protection Planning Requirements. In addition to the protection planning requirements of the PM, the operational command or commands should begin their own protection planning activity early in the acquisition cycle and coordinate this planning with the PM and the SSWG. Operating command security requirements should be added to the program protection plan as part of the lifecycle protection requirements for an acquisition program. This would ensure that the acquisition element and the operational command or commands have similar protection standards and to afford the opportunity for reduction in life-cycle costs through prudent up front investment.

2.9.1. System Security Concept Development.

2.9.1.1. During Mission Area Plan development, security issues for new major acquisition programs should be addressed. The System Security Concept (SSC) is developed using the postulated nuclear and nonnuclear threats and the Security Vulnerability Analysis. System critical characteristics and sensitivity levels to mission capability should be correlated with the national security information categories, intelligence indicators, trusted computer system evaluation criteria, system operating modes, essential communication nodes, physical security criteria, OPSEC, and emissions security. All security disciplines should be evaluated during the development of the SSC.

2.9.1.2. The SSC requirements should be traceable to system specific security vulnerabilities, and should identify those that are mitigated, and those that require a Risk Acceptance Authority (RAA) determination. The SSC should baseline the general requirements for manpower, facilities, and equipment that will be developed in detail as part of the weapon system security standard. In the absence of a weapon system security standard and when a one-of-a-kind, high dollar value item, or potentially dangerous product will be developed, produced, modified, or sustained at a contractor-operated facility and this asset requires more physical security requirements than what is listed in the National Industrial Security Program Operating Manual (NISPOM), a clause identifying the physical security requirements from AFI 31-101 should be developed and placed in the contract.

2.9.1.3. The SSC is a life-cycle document and should be updated as determined by the operational command.

2.9.2. Security Estimates for Manpower, Facilities and Equipment.

2.9.2.1. The System Security Standard (SSS) should be derived from the SSC. The SSC and SSS are normally the responsibility of the operational command. The operational command should request an original protection level or a change to an existing protection level in accordance with AFI 31-101, *Air Force Installation Security Program*. Security manpower, facilities, and equipment should be planned for and included in the Weapon System Security Standard to support the CPI/CSR throughout all life-cycle phases including demilitarization.

2.9.2.2. The System Security Manager and the SSWG should assist the operational command and the PM in determining security manpower, facilities, and equipment needs. Include requirements for security manpower, facilities, and equipment early in the planning process to ensure resources are available when needed.

Chapter 3

SYSTEMS SECURITY ENGINEERING (SSE)

3.1. Purpose. The purpose of SSE is to eliminate, reduce, or control, through engineering and design, any characteristics that could result in the deployment of systems with operational security deficiencies. SSE is an essential element of acquisition system protection and is the vehicle for integrating security into the overall systems engineering process. Engineering and other technically related functions and processes are used to develop and identify CPI, technologies, and systems. Technical engineering processes design, develop, test, and manage anti-tamper features in Air Force programs and weapons systems for as long as the protection is required (e.g., the system is demilitarized, or the technology is approved for release to the public).

3.1.1. During the system's design phase, SSE should identify, evaluate, and eliminate or contain known or potential system security vulnerabilities from deployment through demilitarization.

3.1.2. SSE should consider possible enemy capture of the system.

3.1.3. SSE involves the integration of security considerations into the systems engineering process to ensure the total system is evaluated for known or potential system vulnerabilities, and that the system is cost effectively designed to reduce the probability and severity of all identified vulnerabilities.

3.1.4. SSE should be applied to new developments (including off the shelf and non-developmental items) and to modifications of existing systems to minimize the operational costs of protecting deployed systems.

3.1.5. SSE does *not* provide specific weapons capabilities to counter combat threats.

3.2. Vulnerabilities. PMs should assess their program(s) for security vulnerabilities as soon as possible (before Milestone C) to reduce the likelihood of damage, compromise, or destruction to the system.

3.3. Procedures. Within the SSE construct, PMs should establish procedures to:

3.3.1. Identify security requirements optimizing their integration into a single systems engineering approach.

3.3.2. Tailor individual security disciplines to program development efforts as inexpensively as possible.

3.3.3. Identify threats (e.g., physical, electronic, and intelligence) that can be neutralized or minimized through security engineering design and countermeasures.

3.3.4. Identify necessary actions to minimize or contain system or component vulnerabilities.

3.3.5. Optimize life-cycle security costs, while improving overall survivability of the system or component.

3.4. Operational and Support MAJCOMs, Field Operating Agencies, and Supporting Security Forces Requirements. The Operational and support MAJCOM, field operating agencies, and supporting security forces staffs should provide guidance and assistance as necessary in:

3.4.1. Preparing systems security requirements.

- 3.4.2. Including security requirements in MNS and ORD development.
- 3.4.3. Developing a system security concept as defined in AFPD 63-17 and this instruction.
- 3.4.4. Implementing and overseeing technology or program protection planning and related activities.
- 3.4.5. Coordinating command or agency security requirements for systems scheduled to undergo depot maintenance.
- 3.4.6. Participating in SSWG meetings for technology and acquisition programs, as requested by the TD/PM.
- 3.4.7. Establishing Air Force laboratories security requirements at the direction of the TD.
- 3.4.8. Developing security countermeasures based on threat analyses.
- 3.4.9. Coordinating with other MAJCOMs and agencies to ensure adequate, continuous security arrangements exist.
- 3.4.10. Assessing the security impact of SSE change proposals, deviations, and waivers through the system life-cycle.
- 3.4.11. Establish SSE support to ensure security for systems undergoing maintenance or modification.
- 3.4.12. Assisting in security planning, when requested.

3.5. SSE Approach. The Systems Engineering Management Plan (SEMP) is a top-level management document that describes system engineering tasks.

3.6. SSE Process Tool. See [Attachment 5](#). This process tool is intended for use by government agencies and defense contractors for development of system security engineering criteria and applications as required by the defense acquisition process. It establishes the guidance necessary to implement and manage SSE programs and products.

Chapter 4

SECURITY MANAGEMENT

4.1. General. The Air Force relies on contractors to accomplish much of the work involved with systems acquisition. In terms of Program Protection Planning, contracting concerns focus on two general areas. The most basic is to insure that contractors meet program protection requirements that are applicable to them. Program protection requirements should be identified and documented contractually and the contractors should be monitored to insure compliance. In some cases contractors may also be directly developing or supporting program protection requirements themselves.

4.1.1. The government uses the Request for Proposal (RFP) to negotiate acquisitions. The RFP specifies government objectives/requirements and solicits proposals to satisfy these requirements.

4.1.2. The SOO clearly specifies required development or production work for deliverable goods or services from a contractor and is an element of the RFP.

4.1.3. The RFP and SOO should include specific security requirements that the contractor must satisfy. This includes the documentation of security classification guidance using the DD Form 254, **Contract Security Classification Specification**. Additionally, Contract Data List Requirements should identify classification requirements or distribution limited statements for data products developed in support of the acquisition.

4.1.4. Using command(s) should be involved in the development of the RFP and SOO.

4.1.5. TPP/PPP requirements should be included in the RFP and SOO.

4.2. Contractual Requirements for the Protection of Classified Information. The requirements for the protection of classified information in the hands of industry is established under the National Industrial Security Program (NISP) and are documented in DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*. The Federal Acquisition Regulation (FAR) **4.404a**, mandates that the contracting officer insert FAR 52.204-2 into any solicitation or contract when the contract may require access to classified information.

4.3. Additional Security Requirements. Air Force systems may require additional protection while under the control of a contractor, beyond the basic requirements for the protection of classified information. Not all Air Force systems will require a specific level of protection. The requirements for the protection of Air Force assets by the contractor should be included in the MNS and ORD and should be further defined through the development of the system security concept and included in contract clauses or requirements in the RFP and the PPP. This may require additional security requirements above those listed in the NISPOM. Physical security requirements for protection of Air Force products and systems are located in AFI 31-101, *The Air Force Installation Security Program*. Physical security requirements for sensitive conventional arms, ammunition, and explosives are located in DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives*. Use AFI 31-101 and DoD 5100-76-M as guides for requirements. These tools will provide the format for identifying line items to the contracting officer for physical security requirements to be included in the RFP and contracts. Provide these inputs along with the updated PPP to the contracting officer to ensure the contractor understands the requirements and has the most current program protection planning guidance. Update the PPP as critical program information, technologies, or systems are identified or changed.

4.3.1. PMs should:

4.3.1.1. Establish a SSWG. Identify critical program information, technologies, and or systems. Draft and implement the PPP. Identify, budget, plan and program for all security, intelligence, and counterintelligence requirements during concept and technology development phase and include these in acquisition strategic and planning documentation. Include these requirements throughout the system development and demonstration, production and deployment and operations and support phases. Integrate program protection planning requirements throughout acquisition strategic and planning documentation. Define protection planning requirements for technology transitioning from the laboratory and program protection planning requirements for each acquisition life cycle phase as outlined in the MNS, ORD and PMD. Include program protection planning, system security engineering, anti-tamper and all security requirements in the statement of objectives/work, and other sections of the RFP. Continuously assess CSRs/CPIs conducting risk management analyses on each critical program information, technology, and system balancing the cost of security protective countermeasures against the risk of damage, loss, compromise or destruction of the product while at the laboratory, contractor-operated facility, sustainment, operational or other location.

4.3.1.2. Together with the using command, determine if technologies, systems or products undergoing maintenance or modification require additional security, following the requirements outlined in the technology protection, anti-tamper, or other security sections of the MNS and ORD.

4.3.1.3. Ensure any additional security requirements are identified from the PMD.

4.3.1.4. Use all available intelligence, counterintelligence, and threat information in making decisions.

4.3.1.5. Use risk analysis to establish the scope of additional security requirements.

4.3.1.6. Integrate requirements into the PPP.

4.3.1.7. In coordination with operational commands, plan for additional security requirements during the life-cycle of all acquisitions.

4.3.1.8. Ensure contracting officers specifically address these requirements in the RFP and contract when necessary. Develop program protection planning, system security engineering and security, intelligence and counterintelligence requirements into request for proposal evaluation criteria. Include the evaluation requirement for the contractor to propose life cycle protection and system security engineering costs. Participate in source selection and evaluate proposals as directed by the Source Selection Team.

4.3.1.9. Review the security plans of bidders to ensure they meet solicitation requirements.

4.3.1.10. Inform the contracting officer of the results of the review and, if required, recommend specific changes to the security plan in the solicitation.

4.3.1.11. Ensure the additional security requirements are identified to the Defense Security Service (DSS) Cognizant Security Office or servicing security office assigned to monitor the activity.

4.3.1.12. When additional security requirements are included in a contract, stipulate that the contractor report incidents involving the product to the responsible Contract Administration Office, the DSS Cognizant Security Office, the cognizant SSO when SCI is involved, and the servicing acquisition security specialist.

4.3.2. Operational commands should.

- 4.3.2.1. Identify additional security requirements in the system security concept.
- 4.3.2.2. Review mission need statements and ORDs.
- 4.3.2.3. Review plans for system modifications.
- 4.3.2.4. Support contracting activities.
- 4.3.2.5. Support test activities.

4.3.3. SSWG security, intelligence, and counterintelligence technical experts and laboratory, acquisition, sustainment, and using command functional experts assigned to support Technology Protection Planning or Program Protection Planning should:

- 4.3.3.1. Propose additional security requirements to the using command and/or TD/PM.
- 4.3.3.2. Tailor requirements to the individual contractor facility.
- 4.3.3.3. Prevent duplicate or excessive security requirements and costs.
- 4.3.3.4. Work with the program office and the contracting office to specify which requirements to include in solicitations and contracts. Use the sample list in [Table 4.1](#) as a starting point to identify requirements.

Table 4.1. List of Additional Security Considerations (NOTE 1).

1. Contractor Physical Security Plan
2. Contingency Plan (emergency operations)
3. Operating Instructions
4. Post Instructions
5. Holding area boundary barrier (NOTE 2)
6. Holding area lighting
7. Holding area warning signs
8. Holding area entry controls (NOTE 3)
9. Holding area lighting
10. Holding area entry point lights
11. Holding area internal patrol (NOTE 4)
12. Holding area internal circulation controls
13. Positive product access controls
14. Holding area armed response
15. Holding area badge system (NOTE 3)
16. Intrusion detection system
17. Security force communications
18. Security force training
19. Centralized security force control center
20. Positive identification system (NOTE 3)
21. Key and lock controls

NOTE 1. This is a sample list of security criteria to consider for application to a particular program. Each program is different, so tailor the security guide to the product. Avoid excessive security costs where threat is low or where the product is not critical.

NOTE 2. Walls of rooms or buildings, or fencing.

NOTE 3. Entry controller or automated entry system.

NOTE 4. Excluding rooms and buildings.

4.3.3.5. Evaluate plans received from bidders in response to solicitations.

4.3.3.6. Conduct surveys of contractor's compliance at the request of the TD/PM.

4.3.3.7. Review contractors' responses to problems identified in surveys.

4.3.3.8. Recommend corrective action to the contract administration office when a survey reveals a security problem.

4.3.3.9. Provide general security assistance to program offices as necessary.

4.3.3.10. Ask the MAJCOM for guidance as needed.

4.3.4. The Defense Contract Management Agency International (DCMAI) administers contracts for overseas depot operations. DCMCI should coordinate security surveys with acquisition security specialists, and the overseas MAJCOM.

4.3.5. Security Surveys.

4.3.5.1. The purpose of initial and follow-on surveys is to evaluate the adequacy of additional security requirements outlined in the contract and PPP.

4.3.5.2. Make sure security surveys are cost-effective. Do not conduct surveys where there are other means of evaluating security. Where security requirements are minimal, the PM may authorize the contractor to perform a survey. In these cases, the contractor should provide written certification to the PM of security at the facility.

4.3.5.3. Pre-award Surveys. Pre-award surveys should be used to:

4.3.5.3.1. Ensure the contractor can meet the requirements identified in the solicitation.

4.3.5.3.2. Determine whether the contractor has satisfied the requirements by participating in the Industrial Security Program or some other security program such as Sensitive Compartmented Information or Special Access Required.

4.3.5.3.3. Evaluate the contractor's security plan(s) and physical security measures.

4.3.5.3.4. If the survey identifies problems in the contractor's program, recommend corrections to the contract administration office to be included in the contract.

4.3.5.4. An initial survey should be conducted not later than 90 days after the contract is awarded, and at 2-year intervals thereafter. PMs may vary the 2-year survey cycle if additional surveys are not cost-effective, or if there is a need for more frequent surveys.

4.3.5.5. The contractor and contract administration office should be notified in advance of a proposed survey. However, if security is in question no notice surveys may be used.

4.3.5.6. Security surveys should be addressed to the requesting PM with informational copies to the operational command(s). A copy of the most recent survey should be kept in the security office supporting the program.

4.3.5.7. Security specialists should evaluate corrections that the contractor proposes. If corrective action seems inappropriate, the program office and contracting officer concerned should recommend further action.

Chapter 5

PROGRAM PROTECTION SURVEYS (PPS)

5.1. General. At least one PPS should be conducted on Acquisition Category (ACAT) I and ACAT II acquisition programs containing CPI or CSR during each phase of the acquisition cycle. The PPS can be used to assess the effectiveness of the established program protection following PPP approval and implementation. Use the list in [Table 4.1.](#) and the PPP to plan and conduct a PPS. The PPS should be the PM's primary tool to evaluate and validate the PPP.

5.2. PPS Objectives.

- 5.2.1. Assess the overall effectiveness of the PPP during a given phase.
- 5.2.2. Provide specific indicators of possible losses of CPI/CSR.
- 5.2.3. Provide specific information on how the loss of CPI/CSR occurred.
- 5.2.4. Provide information to update the PPP for the remaining phases.
- 5.2.5. Identify potential critical infrastructure vulnerabilities to determine how to mitigate them.

5.3. Purpose. The PPS provides the PM with information about the effectiveness of the security applied to the program. Based on this information, the PM may continue the PPP as written, or refocus resources to eliminate any security short falls.

- 5.3.1. Determine if the previously identified CPI/CSR received adequate protection during a given phase. Focus on specific threats and countermeasures.
- 5.3.2. Limit the survey to determine the effectiveness of the protection and countermeasures planned and implemented at a specific facility to protect the CPI/CSR of a selected program. The survey methodology is to reproduce an adversary's approach to the program being assessed, not to assess compliance with security procedures.
- 5.3.3. A written report should be provided to the PM addressing, as a minimum:
 - 5.3.3.1. Effectiveness of the protection measures applied to the program's CPI/CSR.
 - 5.3.3.2. Recommendations to improve protection measures to eliminate or reduce vulnerabilities.
- 5.3.4. The PPS should not be used as an inspection and should not be graded. To obtain accurate information and be a successful tool, the PPS team depends on positive cooperation and assistance from the program management organization and the facility being surveyed.
- 5.3.5. The PPS report should be provided only to the PM. Any further distribution should be done only with PM approval. PMs should retain official file copies of each survey conducted.
- 5.3.6. Along with the PPS report, the PPS team chief should provide a "lessons learned" report to the PM discussing specific areas of PPP strengths and weaknesses. This report should be an abbreviated discussion omitting actual locations, personal names and other program identifying information. This report should:
 - 5.3.6.1. Be correlated against common trends and/or problems in the technology/acquisition community.

5.3.6.2. Concentrate on generic problems with resources, facilities, and/or training.

5.3.7. A PPS should not be conducted at contractor-owned or operated locations unless the provisions of the contract authorize compliance inspections. Surveys should be coordinated with the servicing government security oversight office.

5.4. Information Collections, Records, and Forms.

5.4.1. Information Collections. No information collections are created by this publication.

5.4.2. Records. No Records are created by this publication

5.4.3. Forms Prescribed.

5.4.3.1. Adopted Forms. DD Form 254, **Contract Security Classification Specification**.

5.4.3.2. Prescribed Forms. No forms are prescribed by this publication.

MARVIN R. SAMBUR
Assistant Secretary of the Air Force for Acquisition

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives*

DoD 5200.1-H, *Department of Defense Handbook for Writing Security Classification Guidance*

DoD 5200.1-M, *Acquisition Systems Protection Program*

DoD 5200.1-R, *Information Security Program*

DoD Directive 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*

DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*

DoD Regulation 5400.7/Air Force Supplement, *DoD Freedom of Information Act Program*

DoD Directive 8500.1, *Information Assurance (IA)*

AFPD 63-17, *Technology and Acquisition Systems Security Program Protection*

AFI 10-1101, *Operations Security*

AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations* (Confidential)

AFI 31-101, *The Air Force Installation Security Program* (FOUO)

AFI 31-401, *Information Security Program Management*

AFI 33-202, *Computer Security*

AFI 33-203, *Emission Security*

AFI 63-1201, *Assurance Of Operational Safety, Suitability, & Effectiveness*

AFMAN 37-139, *Records Disposition Schedule*

Air Force Anti-Tamper Security Classification Guide

Abbreviations and Acronyms

ACAT—Acquisition Category

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFRL—Air Force Research Laboratory

AIS—Automated Information Systems

ASAF(A)—Assistant Secretary of the Air Force (Acquisition)
ASR—Alternate System Review
AT—Anti-Tamper
C4I—Command, Control, Communications, Computers, and Intelligence
CDR—Critical Design Review
CDRL—Contract Data Requirements List
CI—Counterintelligence/Configuration Item
CIP—Critical Infrastructure Protection
CISP—Counterintelligence Support Plan
CM—Configuration Management
CNWDI—Critical Nuclear Weapons Design Information
COCO—Contractor Owned Contractor Operated
COMPUSEC—Computer Security
COMSEC—Communications Security
CONOPS—Concept of Operations
CPI—Critical Program Information
CSR—Critical System Resource
CTTA—Certified TEMPEST Technical Authority
CWBS—Contract Work Breakdown Structure
DAA—Designated Approving Authority
DCMAI—Defense Contract Management Command International
DDL—Delegation of Disclosure Authority Letter
DID—Data Item Description
DoD—Department of Defense
DoDISS—Department of Defense Index of Specifications and Standards
DT&E—Developmental Test and Evaluation
DSS—Defense Security Service
FAR—Federal Acquisition Regulation
FCA—Functional Configuration Audit
FOIA—Freedom of Information Act
GOCO—Government Owned Contractor Operated
INFOSEC—Information Security

ISPM—Information Security Program Manager
ISS—Information Systems Security
IT&S—Information, Technologies, and Systems
MAIS—Major Automated Information System
MAJCOM—Major Command
MDA—Milestone Decision Authority
MDAP—Major Defense Acquisition Program
MNS—Mission Needs Statement
NATO—North Atlantic Treaty Organization
NISP—National Industrial Security Program
NISPOM—National Industrial Security Program Operating Manual
NTIS—National Technical Information Service
OPR—Office of Primary Responsibility
ORM—Operational Risk Management
ORD—Operational Requirements Document
OPSEC—Operations Security
OT&E—Operational Test and Evaluation
PDR—Preliminary Design Review
PM—Program Manager
PMD—Program Management Directive
PPP—Program Protection Plan
PPS—Program Protection Survey
PWBS—Program Work Breakdown Structure
RAA—Risk Acceptance Authority
RCM—Requirements Correlation Matrix
RDT&E—Research, Development, Test, and Evaluation
RFP—Request for Proposal
RTP—Research and Technology Protection
S&T—Science and Technology
SAP—Special Access Program
SCG—Security Classification Guide
SCI—Sensitive Compartmented Information

SE—Systems Engineering

SEMP—Systems Engineering Management Plan

SFR—System Functional Review

SIOP-ESI—Single Integrated Operational Plan - Extremely Sensitive Information

SOO—Statement of Objective

SPO—System Program Office

SRR—System Requirements Review

SSC —System Security Concept

SSE—System Security Engineering

SSEM—System Security Engineering Management

SSS—System Security Standard

SSWG—System Security Working Group

STA—Security Threat Analysis

STAR—System Threat Assessment Report

ST&E—Security Test and Evaluation

STOA—Security Trade Off Analysis

SVA—Security Vulnerability Analysis

TA/CP—Technology Assessment/Control Plan

TCB—Trusted Computing Base

TD—Technology Director

TEMP—Test and Evaluation Master Plan

TEMPEST—Technical Electro-Magnetic Pulse Emanation Suppression Techniques

TPP—Technology Protection Plan

USD (AT&L)—Under Secretary of Defense for Acquisition, Technology, and Logistics

WBS—Work Breakdown Structure

Terms

Anti-Tamper (AT)—Anti-Tamper is defined as the systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems.

Counterintelligence Support Plan (CISP)—The CISP is a formally coordinated action plan for CI support to protect research and technology at specific DoD research, development, test, and evaluation facilities and acquisition programs. The plan addresses key aspects of the installation, the activity or program, and the nature of the CI activities to be employed. A separate plan may be prepared for each DoD contractor or academic institution where CPI or CSR are involved.

Critical Infrastructure Protection (CIP)—The identification, assessment, protection and real-time monitoring of cyber & physical mission critical infrastructures essential to the execution of the National Military Strategy.

Critical Program Information (CPI)—CPI is program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such critical programs, technologies, or systems.

Contractor Owned/Contract Operated (COCO)—An industrial facility owned and operated by a contractor.

Critical System Resources (CSR)—In an acquisition or operational program, those resources, for which the loss, theft, destruction, misuse, or compromise would damage current or future US war-fighting capability. CSR includes, but is not limited to, single critical failure nodes, extremely high-cost items, politically sensitive material, etc.

Government Owned/Contractor Operated (GOCO)—An industrial facility owned by the government, but operated by a contractor.

Infrastructure—A framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole.

Mission Needs Statement (MNS)—A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept and Technology Development Phase of Pre-Systems Acquisition.

Operational Requirements Document (ORD)—A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or the user's representative at each milestone beginning with Milestone I, Concept Demonstration Approval of the Requirements Generation Process.

Operational Risk Management (ORM)—The systematic process of identifying hazards, assessing risk, analyzing risk control options and measures, making control decisions, implementing control decisions, accepting residual risks, and supervising/reviewing the activity for effectiveness.

Program Manager (PM)—The individual designated by an Air Force Acquisition Executive to manage an acquisition program, and appropriately certified under the provisions of the Defense Acquisition Workforce Improvement Act (10 U.S.C. § 1701 et seq).

Program Management Directive (PMD)—The official Air Force document used to direct acquisition responsibilities to the appropriate major commands, agencies, program executive office, or designated acquisition commander. All acquisition programs require PMDs.

Program Protection Planning—An acquisition and logistics managed program process that identifies a system's critical program elements, threats, and vulnerabilities throughout the system's life-cycle. Program Protection Planning is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment, and facilities.

Science and Technology (S&T) Program—The S&T program is an integrated set of programs that are an Air Force corporate investment for the future. S&T includes basic research, applied research, and advanced technology development to produce generic, not system-specific, technologies. Neither a validated requirement nor programmed funding for formal acquisition is necessary to begin an S&T effort.

Sensitive Compartmented Information (SCI)—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DoD 5200.1-R, *Information Security Program*.)

Special Access Program (SAP)—A sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.

System Program Office (SPO)—The office of the PM and the single point of contact with industry, government agencies, and all other life-cycle activities throughout the systems acquisition and sustainment processes.

System Security Engineering (SSE)—An element of system engineering that applies scientific and engineering principles to identify and reduce system susceptibility to damage, compromise, or destruction; and the identification, evaluation, and elimination or containment of system vulnerabilities to known or postulated security threats in the operational environment.

System Security Management Plan—A formal document that fully describes the planned security tasks required to meet system security engineering requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering, design and management activities, and related systems.

Technology Director (TD)—The Air Force Research Laboratory (AFRL) is one laboratory made up of multiple technology directorates. A single “Director,” who is responsible for the technology programs that occur at their particular directorate, leads each technical directorate.

Technology Protection Plan (TPP)—Similar to the PPP developed in the acquisition cycle, a TPP is developed by research organizations that identify critical technology (e.g., breakthrough technology) requiring increased protection.

Attachment 2

**MEMORANDUM FROM THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY, AND LOGISTICS, RESEARCH AND TECHNOLOGY - PROTECTION
PROGRAM PLANS, 30 JUNE 2000****THE UNDER SECRETARY OF DEFENSE****3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010****JUN 30 2000****MEMORANDUM FOR SERVICE ACQUISITION EXECUTIVES
DIRECTOR, ACQUISITION RESOURCE ANALYSIS****SUBJECT: Research and Technology Protection – Program Protection Plans**

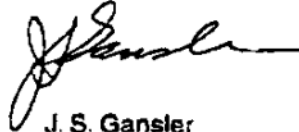
On February 17, 2000, the Deputy Secretary of Defense signed five memoranda directing major enhancements in the Department's technology protection programs. Initiatives described in the February 17 memoranda were addressed by an overarching integrated process team (OIPT) chartered by the Deputy Secretary of Defense in response to a DoD Inspector General (IG) report that identified practices that could benefit from improvement. The DoD IG report documented the failure of many acquisition program managers managing critical program information (CPI) to notify their servicing CI organizations in order to obtain support in accordance with DoD guidance.

In accordance with the recommendations of the OIPT, we will work with ASD(C3I) to revise DODD 5200.39 and other appropriate directives to strengthen requirements for program manager training for Research, Development, Test and Evaluation (RDT&E) technology protection plans and program protection plans. We will also take appropriate steps to establish security as an equal partner for acquisition programs with cost, schedule, and performance. I am advocating an approach that will result in increased emphasis on program manager accountability for successful execution of program protection plans within normal reviews of acquisition programs. Consequently, I am directing the following actions:

- a. Service Acquisition Executives shall increase emphasis to ensure development and implementation of an improved program protection plan process and successful execution of program protection plans.
- b. The Defense Acquisition Board (DAB) Secretariat shall ensure that development and execution of program protection plans are included in the DAB review process.



Accomplishments will be tracked through the OIPT, which will meet regularly to review initiatives and prepare progress reports. Report your progress in implementing this direction within 60 days of the date of this memorandum to the OIPT Action Officer, Ms Vicki Cox, ODUSD (S&T), 703-697-9215. Please contact her if you have any questions.



J. S. Gansler

cc:
ASD(C31)

Attachment 3**THE SYSTEM SECURITY WORKING GROUP (SSWG)**

A3.1. Organization . The SSWG is a working forum of functional experts who support the security, intelligence, and counterintelligence needs of the technology project or any acquisition, modification or sustainment program for the TD or PM. The size and nature of the project, program or system will dictate the size and makeup of the SSWG. A SSWG should be formed for all projects and programs that contain critical scientific research technologies or critical program information, technologies, and/or systems and should include but is not limited to functional representation from the below listed areas.

- A3.1.1. Laboratory Project Office/System Program Office.
- A3.1.2. Chief or Senior Engineer.
- A3.1.3. Chief or Senior Scientist.
- A3.1.4. Acquisition Security.
- A3.1.5. Information Security.
- A3.1.6. Industrial Security.
- A3.1.7. Personnel Security.
- A3.1.8. Physical Security.
- A3.1.9. Foreign Disclosure.
- A3.1.10. Communications Security.
- A3.1.11. Operations Security.
- A3.1.12. Logistics.
- A3.1.13. Information Assurance.
- A3.1.14. Counterintelligence.
- A3.1.15. Intelligence.
- A3.1.16. Scientific and Technical Information Office.
- A3.1.17. Special Security Office (where applicable).
- A3.1.18. Special Access Program Representative (where applicable).
- A3.1.19. Operational command(s).
- A3.1.20. Contracting.
- A3.1.21. Financial Management.
- A3.1.22. Test Management.
- A3.1.23. Other functional experts, as required.

A3.2. The SSWG Roles and Responsibilities.

A3.2.1. Should be established by the TD or PM and be chaired by the TD/PM, Chief Scientist or Chief Engineer.

A3.2.2. Should develop a charter.

A3.2.3. Should identify SSWG team members and participants

A3.2.4. Should evaluate the modernization planning requirements documents, MNS, ORDs, and PMDs. Evaluate each requirements document outlining the technology/program protection planning requirements for the completion of each section of the program protection plan.

A3.2.5. Should assist in the preparation of the following documents and material:

A3.2.5.1. Program Protection Plan

A3.2.5.2. Security Threat Analysis

A3.2.5.3. Systems Vulnerability Analysis

A3.2.5.4. System Security Concept

A3.2.5.5. System Security Management Plan

A3.2.5.6. Vulnerability Countermeasures

A3.2.5.7. Security Classification Guide(s)

A3.2.6. Should evaluate each system security engineering, security, intelligence, and counterintelligence process (i.e., system security engineering, anti-tamper, computer security, communications security, operations security, information security, information protection, industrial security, personnel security, physical security, antiterrorism/force protection, international program and other security requirements identified by the using command).

A3.2.7. Should identify the make-up of the SSWG and the functional experts needed by the TD or PM to have viable technology/program protection planning.

A3.2.8. As technology and acquisition strategies and program documentation is compiled, it should integrate the protection and security requirements.

A3.2.9. As technologies and system concepts are functionally decomposed, the scientists and engineers should identify what is CSR/critical program information, technologies and/or systems (CPIs) and obtain approval from the PM.

A3.2.10. Once CSR/CPI is identified and approved by the PM, or breakthrough technology by the TD, they should be protected.

A3.2.11. Should determine if they are controlled unclassified information or classified CSR or CPIs. Classified must follow the information security rules outlined in DoD 5200.1-R and AFI 31-401.

A3.2.12. Should provide the list of CSR/CPIs to Air Force Office of Special Investigation (AFOSI). Request a multi-disciplinary counterintelligence threat assessment be conducted.

A3.2.13. When PM approves the CSR/CPI, the PPP should be developed or updated.

A3.2.14. AFOSI delivers threat assessment. The SSWG should meet to review the threat data and determine the risk to the identified CSR/CPI.

A3.2.15. Scientists and engineers should determine if protective measures need to be designed into the systems architecture through systems engineering, if anti-tamper features need to be developed or if a requirement that exists in one of the security programs could be applied and used as a protective measure. Whichever protective countermeasure is used, it should be developed into the test plan and verified that the protective countermeasure selected functions as designed to protect the system from being damaged, destroyed, compromised, or lost before it is delivered to the warfighter.

A3.2.16. Should determine if other programs have like technologies or systems and determine if they are protecting them equivalent to your program.

A3.2.17. If not, it should coordinate with the program office or service organization to resolve any protection discrepancies with the outcome of protecting like technologies in the same manner.

A3.2.18. If a protection issue exists and no resolution is obtained at the working level, it should elevate the issue through the proper chain of command.

A3.2.19. Should update the PPP, educate and notify project/program/contractor personnel that work with CSR/CPI that changes have occurred to the PPP. Keep them informed and continuously aware of the importance of protecting CSR/CPIs .

A3.2.20. Should develop critical information lists and inform personnel on what is and is not information that can be revealed outside of the organization. Establish an OPSEC program to prevent an adversary from reaching your CSR/CPIs. Keep the latest information updated in the PPP.

A3.2.21. Should propose additional, incomplete, or security issues that require clarification by the using command or other organizations to the PM.

A3.2.22. Scientists and engineers should determine if a system security design-in needs to be developed into the systems architecture; decide if an anti-tamper feature needs to be developed; or determine if an existing security protective process in one of the security programs established as a requirement will adequately protect the CSR/critical information, technology and/or system.

A3.2.23. Should also include those listed in [4.3.3.2.](#) through [4.3.3.10.](#)

A3.3. Chairman. The PM or PM's designee should chair the group.

A3.4. Membership. Membership should not be arbitrarily limited. Include representatives from any organization that can directly contribute to the system security development. Consider including non-Air Force organizations and agencies that create military component or national-level policies affecting system security.

Attachment 4

SECURITY WORK BREAKDOWN STRUCTURE (WBS)

A4.1. General.

A4.1.1. **Purpose.** The purpose of this attachment is to provide both government and industry with a framework for tracking and reporting program security costs. It may also be used to estimate life-cycle security costs. The WBS should be prepared in accordance with the guidance in MIL-HDBK-881.

A4.1.1.1. The WBS is a management technique used to divide a program or project into manageable elements reflecting all products to be delivered and services to be performed. It relates the elements of work to be accomplished to each other and to the end product. It is a product-oriented family tree composed of hardware, software, services, data, and facilities. This family tree results from systems engineering efforts during the acquisition of a defense materiel item.

A4.1.1.2. The Program WBS (PWBS) consists of all efforts required to complete the total system. The PWBS is composed of all contract WBS (CWBS) elements coupled with in-house WBS elements related to the development and/or production of the specific defense materiel item. The PWBS consists of at least three levels of WBS elements, as prescribed by MIL-HDBK-881.

A4.1.1.3. The CWBS is the complete WBS for a specific contract. The program office structures the preliminary CWBS using elements from the PWBS that are applicable to the specific contract. The final CWBS is negotiated between the contractor and the program office. The CWBS provides a direct link between the contracted effort and the total project.

A4.1.1.4. The Systems Security Engineering Manager should be involved during the preparation of the Program WBS and the Preliminary CWBS to ensure program protection planning, system security engineering, and product security elements are integrated.

A4.1.2. Costs.

A4.1.2.1. Costs should be reported under the following categories. Descriptions for each category may be found in Section II of this attachment.

A4.1.2.1.1. Program Protection Planning.

A4.1.2.1.2. System Security Engineering.

A4.1.2.1.3. Additional security requirements for contracts.

A4.1.2.1.4. Program Security Management.

A4.1.2.2. Follow established policy when apportioning resources that support both security and non-security activities. If no policy exists, resources should be estimated to the nearest 5 percent. Use the same method when apportioning and reporting resources that support two or more security activities or two or more contracts.

A4.1.2.3. Within the cost accounting structure, Program Protection Planning and Systems Security Engineering costs should be aggregated at both the systems and component levels (e.g., avionics, airframe, propulsion, etc.), as appropriate. Program Security Management costs should be aggregated only at the systems level.

A4.1.2.4. Report security costs as cost reporting deliverables dictate.

A4.2. Descriptions:

A4.2.1. Program Protection Planning . Program protection planning involves the identification and safeguarding of systems, components, and technical data anywhere from Systems Acquisition through the Sustainment processes. This includes technologies being developed, support systems (e.g., test and simulation), and research data with military or space applications.

A4.2.1.1. Identification of CPI and CSR. See paragraph [2.7.2.3](#) of this instruction.

A4.2.1.2. Development and implementation of countermeasures. See paragraph [2.7.2.9](#) of this instruction.

A4.2.1.3. Development and implementation of anti-tamper measures. See paragraph [2.7.2.10](#) of this instruction.

A4.2.1.4. Administration (to include government and contractor costs). Administration and overhead costs not included in other subcategories.

A4.2.1.5. Operational, Test and Evaluation.

A4.2.1.6. Operations Security. See AFI 10-1101, Attachment 7.

A4.2.1.7. Foreign Disclosure. See paragraph [2.7.2.13](#) of this instruction.

A4.2.2. System Security Engineering. System Security Engineering applies scientific and engineering principles through the systems engineering process to identify and reduce systems susceptibility to damage, compromise, or destruction. It identifies, evaluates, and eliminates or contains system vulnerabilities to known or postulated security threats in the operational environment. This involves developing security requirements into the systems security engineering architecture. Activities include, but are not limited to the identification of Information, Technologies, and Systems (IT&S), developing system security concepts, conducting threat and vulnerability analysis, security risk analysis, conducting trade studies, identifying security alternatives, determining life-cycle security costs, and developing security countermeasures to provide continuous program protection. Contractors shall limit their security cost reporting to those security cost categories directly associated with these activities.

A4.2.2.1. Production and deployment transition costs. Costs directly attributable to contracted production, and those required for the transition of production item from the contractors control to the government. The government will report transition costs from the government to the contractor.

A4.2.2.2. Administration (to include government and contractor costs). Administration and overhead costs not included in other subcategories.

A4.2.2.3. Demilitarization.

A4.2.3. Additional Security Requirements.

A4.2.3.1. Security costs specifically associated with COCO/GOCO facilities.

A4.2.3.2. Follow-On Support and Modification costs including both those incurred due to the follow-on support and/or modification process, and those incurred afterward as a result of the work performed.

A4.2.3.3. Administration (to include government and contractor costs). Administration and overhead costs not included in other subcategories.

A4.2.4. Program Security Management. Program Security Management documents those resources expended in safeguarding and securing program information, materials, technologies, and systems. Costs should be aggregated and reported in the following subcategories.

A4.2.4.1. Personnel Security. Those activities associated with determining a person's eligibility and/or suitability for access to classified and/or sensitive information, and access to controlled and/or restricted areas. This includes processing clearance requests, conducting investigations, adjudicating eligibility and/or suitability, and maintaining access and clearance records systems.

A4.2.4.2. Physical Security. Measures designed to safeguard and protect personnel, information, materials, systems, and facilities. This includes security equipment, guard forces, intrusion detection alarm systems, security aids (e.g., fences, lights, etc.), access control and badging systems, and visitor control.

A4.2.4.3. Information Security. This includes the following resources.

A4.2.4.3.1. Information Management. The identification, control, transfer, transmission, classification, declassification, marking, and destruction of classified and/or sensitive information.

A4.2.4.3.2. Automated Information Systems (AIS). The measures and controls implemented to ensure confidentiality, integrity, and availability of information stored within a computer, information system, or network.

A4.2.4.3.3. COMSEC. The measures and controls used to deny access of unauthorized persons to sensitive and/or classified telecommunications information.

A4.2.4.3.4. OPSEC. The actions taken to identify and deny access to sensitive information that may reveal capabilities and/or intentions.

A4.2.4.3.5. COMPUSEC. The actions taken to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle.

A4.2.4.4. Security Education, Training, and Awareness. The resources devoted to the administration and support of an education, training and awareness function (e.g. instructors/trainers, materials, facilities, training aids, records maintenance).

A4.2.4.5. Special Access Programs. This includes resources in direct support of establishment and administration of additive safeguards and standards (e.g., Special Compartmented Information (SCI), Critical Nuclear Weapons Design Information (CNWDI), Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI), and North Atlantic Treaty Organization (NATO) information). This incorporates elements of all other subcategories.

A4.2.4.6. Industrial Security. Guidance and oversight to contractors performing on Air Force classified contracts. This includes Federally Funded Research and Development Centers and Contract Employee Technical Assistance personnel.

A4.2.4.6.1. Review and validation of requirements in DD Form 254, **Contract Security Classification Specification**.

A4.2.4.6.2. Assistance in preparation of security requirements for Statement of Objectives and Statement of Work.

A4.2.4.6.3. Development of security procedures for contractors performing work on Air Force installations.

A4.2.4.6.4. Issuance of necessary credentials for installation and area access.

A4.2.4.6.5. Performance of oversight inspections in accordance with governing directives and agreements.

A4.2.4.6.6. Providence of security education, training, and awareness support in accordance with governing directives and agreements.

A4.2.4.6.7. Determining security manpower, equipment, and facility costs for corporate research activities.

A4.2.4.7. Administration (to include government and contractor costs). Administration and overhead costs not included in other subcategories.

Attachment 5**SYSTEM SECURITY ENGINEERING PROCESS TOOL**

SYSTEM SECURITY ENGINEERING
PROCESS TOOL



FOREWORD

1. This process tool is intended for use by government agencies and defense contractors for development of system security engineering criteria and applications as required by the defense acquisition process. It establishes the guidance necessary to implement and manage SSE programs and products. This process tool is intended to be used as a stand alone, non-directive guide. Provisions in this process tool should be tailored to the specific product or system being acquired when developing a statement of objective (SOO), request for proposal (RFP), or other document used in contracting for products and systems. System Security Engineering (SSE) is applied throughout the system life-cycle as an element of the system engineering process to provide a comprehensive, iterative, systems approach which:

- a. Uses systems engineering principles to minimize or contain defense systems vulnerabilities to known or postulated security threats in the system's operational environment, during peacetime or increased international tension.
- b. Identifies vulnerabilities, characterizes security risks to the system in the operational environment, develops risk mitigation approaches and a comprehensive security risk management program.
- c. Translates an operational need into a set of technical system security design requirements applied through system development, manufacturing, verification, deployment, operations, support, training, and disposal.
- d. Reduces technical acquisition risks through early identification of requirements, costs, and demonstration of security effectiveness through test and evaluation during systems design and development activities.

2. This process tool defines the SSE process to integrate security in systems acquisition program design and development. The SSE process establishes a single security risk management approach and provides the government with a methodology to evaluate progress in achieving system security objectives for physical security systems and for Information System Security (ISS), which includes control of compromising emanations (TEMPEST), Communications Security (COMSEC), and Computer Security (COMPUSEC). The integration of system security engineering is accomplished through:

- a. development of system products and processes to identify and satisfy user security needs;
- b. utilization of multi-disciplined security teams; and
- c. integration of multi-security program requirements into a single security risk management process.

TABLE OF CONTENTS

<u>Paragraph</u>		<u>Page</u>
A5.1.	SCOPE	49
A5.1.1.	Purpose	49
A5.1.2.	Authority	49
A5.1.3.	Applicability	49
A5.1.4.	Tailoring Application Guidance	49
A5.2.	APPLICABLE DOCUMENTS	49
A5.2.1.	Government Documents	49
A5.2.2.	Order of Precedence	50
A5.3.	DEFINITIONS AND ACRONYMS	50
A5.3.1.	Definitions	50
A5.3.2.	Acronyms	50
A5.4.	GENERAL REQUIREMENTS	50
A5.4.1.	System Security Engineering (SSE)	50
A5.4.2.	System Security Engineering in the Acquisition Phases	51
A5.5.	DETAILED REQUIREMENTS	55
A5.5.1.	System Security Engineering Requirements	55
A5.5.2.	Security Organization	59
A5.5.3.	System Security Working Groups	59
A5.5.4.	Configuration Management	60
A5.5.5.	SSE Data Requirements	60
A5.6.	NOTES	60
A5.6.1.	Intended Use	60
A5.6.2.	Acquisition Requirements	60
A5.6.3.	Consideration of Data Requirements	60

Figure

A5.1.	System Security Engineering Process Application Model	57
-------	---	----

Appendix

A5A.	GLOSSARY	61
A5B.	ACRONYMS	66

A5.1. Scope.

A5.1.1. Purpose. This document prescribes integration methodology and engineering process standards for the identification and implementation of system security requirements into the Air Force's technology projects and acquisition of operational systems. System security engineering should be applied to new developments (including off-the-shelf and non-developmental items) and to modifications of new or existing systems: Equipment and facilities to minimize the system's vulnerabilities to adversarial actions and operational costs of protecting the deployed system throughout sustainment and until demilitarization of the system. While this process tool is primarily a contracting tool for compliance purposes and statement-of-work tasking, government activities can also use it as a model for integrating system security engineering requirements into system specifications and design activities.

A5.1.2. Authority. The DoD 5000-series of publications, DoD 5200.1-M, *Acquisition Systems Protection Program*, and AFPAM 63-1701, *Program Protection Planning*, establish a disciplined approach for acquiring systems and materiel that satisfies the operational users needs, except when statutory requirements override.

A5.1.3. Applicability. This process tool applies to each defense acquisition program during pre-milestone A (Pre-Concept & Technology) development activities and each phase of the acquisition process. Tasks and requirements described in this process tool should be tailored to system acquisition contract specifications, requirements documents, requests for proposal, statements of work, and government in-house efforts with secure operational considerations. For this process tool, the definition of "contractors" includes Government activities developing military systems, equipment and facilities without the involvement of commercially contracted vendors.

A5.1.4. Tailoring application guidance. System Security Engineering application should be based on the system's politico-military value, limited number, or cost. This process tool applies to both the initial design of new or modifications to existing facilities or systems. It is intended to be used as a "model document" to describe the overall basic requirements and activities of a full scale procurement under optimal and normal procurement circumstances. In some instances, a system's procurement may vary due to specific acquisition phases and because of specific interfaces with other on-going program activities. Tasks and activities should be selected which can materially aid in attaining overall security objectives in a cost effective manner. Once selected, the security discipline tasks should be carefully tailored to the specific needs of the program, where separate software development facilities and Automated Information Systems (AIS) are acquired in support of the end system, this guidance must be broadened to include system security engineering planning, risk analysis, system security certification and accreditation of the facility and AISs throughout their life-cycle until demilitarization.

A5.2. Applicable Documents.

A5.2.1. Government documents.

A5.2.1.1. Specifications, standards and handbooks. The following standards form a part of this document to the extent specified herein. Unless otherwise specified, the issue of this document is that listed in the issue of the Department of Defense Index of Specifications and Standards (DoDISS) and supplement thereto, cited in the solicitation (see [A5.6.2.](#)).

A5.2.1.1.1. MIL-HDBK-881, Work Breakdown Structures for Material Items.

A5.2.1.1.2. MIL-STD-882, System Safety Program Requirements.

A5.2.1.1.3. MIL-STD-973, Configuration Management.

A5.2.1.1.4. DoD-STD-2168, Defense System Software Quality Program.

A5.2.1.1.5. ISO/IEC 12207, J-STD-0162.2/Institute of Electrical and Electronic Engineers P1448/EIA PN3764 (U.S. implementation of ISO/IEC 12207).

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from Defense Printing Service Detachment Office, Bldg. 4D, NPM-DoDSSP, 700 Robbins Avenue, Philadelphia PA 19111-5094.)

A5.2.1.2. Other Government documents. The following other Government documents form a part of this process tool to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

A5.2.1.2.1. DoD 5200.1-M, *Acquisition Systems Protection Program*.

A5.2.1.2.2. DoD Directive 8500.1, *Information Assurance (IA)*.

A5.2.1.2.3. DoD 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*.

A5.2.1.2.4. AFPD 63-17, *Technology And Acquisition Systems Security Program Protection*.

A5.2.1.2.5. AFI 33-203, *Emission Security*.

(Unless otherwise indicated, copies are available from National Technical Information Service (NTIS), 5285 Port Royal Rd, Springfield VA 22161.)

A5.2.2. Order of precedence. In the event of a conflict between this text and the documents cited in paragraph [A5.2.1.1](#) above, the text of this process tool takes precedence. In the event of conflict between the text of this process tool and the referenced DoD documents cited in paragraph [A5.2.1.2](#) above, the text of the cited DoD document takes precedent. Nothing in this process tool, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

A5.3. Definitions and Acronyms.

A5.3.1. Definitions. For the purpose of this process tool, the definitions and terms found in Appendix A to this process tool apply.

A5.3.2. Acronyms. For the purpose of this process tool, the definitions and terms found in Appendix B to this process tool apply.

A5.4. General Requirements.

A5.4.1. System Security Engineering (SSE). The tasks detailed in this section should be applicable throughout the system life cycle for any new acquisition program, upgrade, modification, resolution of deficiency, or technology development. The SSE activities should fully consider multi-security discipline requirements and developmental processes and integrate them as a single "functional" requirement. The application of these individual disciplines should be tailored to the program development efforts in the most cost effective manner possible. External and internal organizational and functional interfaces should assure interdisciplinary and engineering integration.

A5.4.2. System security engineering in acquisition phases. SSE activities should be closely related to and dependent upon the acquisition phases and milestone review structure. SSE efforts should be integrated as functional engineering tasks with the systems engineering requirements.

A5.4.2.1. Concept and Technology Development. The following should be planned for by the Government and should directly support the companion systems engineering activities performed in preparation for the Milestone A Decision Authority Review and subsequent phase approval:

A5.4.2.1.1. Early planning-participant identification.

A5.4.2.1.2. Mission Needs Statement (MNS), integrating security capability needs.

A5.4.2.1.3. Technology Protection Plan (TPP) or Program Protection Plan (PPP).

A5.4.2.1.4. System Threat Assessment Report (STAR).

A5.4.2.1.5. System Security Working Group (SSWG).

A5.4.2.1.6. Security Classification Guide (time phased and event driven).

A5.4.2.1.7. Computer System Security Certification and Accreditation.

A5.4.2.1.8. System Concept Studies to identify key concepts.

A5.4.2.1.9. Security Threat Analysis (STA). Compare results of System Threat Assessment Report and TPP breakthrough technology or PPP Critical Program Information (CPI) or Critical System Resources (CSR).

A5.4.2.2. Concept & Technology Development Phase.

A5.4.2.2.1. Update the STA.

A5.4.2.2.2. Identify key system components, software, AIS/hardware, facilities, communications and operational procedures using system description and System Concept Studies. (Review CPI/CSR section of PPP.)

A5.4.2.2.3. Develop System Vulnerability Analysis (SVA). Use PPP, CPI/CSR, STAR and STA.

A5.4.2.2.3.1. Document system security vulnerabilities and value to adversaries.

A5.4.2.2.3.2. Identify impacts to sensitivity or criticality of mission success in deployment.

A5.4.2.2.4. Identify system certification and accreditation requirements and agencies.

A5.4.2.2.5. AIS (commonly referred to as computer systems) should have independent certification and Designated Approving Authority (DAA) accreditation requirements.

A5.4.2.2.6. Determine SSE measures and concepts to assure integrity, availability and confidentiality as outlined in the System Security Concept.

A5.4.2.2.7. Participate in Alternate System Review (ASR).

A5.4.2.3. System Development & Demonstration Phase. The Government System Program Office (SPO) should continue the integration of system security engineering processes through development of:

A5.4.2.3.1. System Security Engineering Baseline. Define/refine system security engineering baseline elements.

A5.4.2.3.1.1. Update/refine system security engineering plans and documentation from the previous phase.

A5.4.2.3.1.2. Define/refine system security engineering and subsystems specifications.

A5.4.2.3.1.3. Update/refine System Security Management Plan and SSC.

A5.4.2.3.1.4. Update/refine the Security Vulnerability Analysis and System Security Engineering Management Program, integrating the information into the various system engineering plans.

A5.4.2.3.1.5. Update/refine the PPP, integrating the information into the system security engineering requirements.

A5.4.2.3.1.6. Identify Product Security requirements.

A5.4.2.3.1.7. Conduct Cost, Benefit Analysis and Trade Studies.

A5.4.2.3.1.8. Develop the Automated Information Systems (AIS) Security Plan, Technical Electro-Magnetic Pulse Emanation Suppression Techniques (TEMPEST) Data Package and manpower impact assessments.

A5.4.2.3.1.9. The system security engineering requirements and constraints should be developed as part of the system's allocated configuration baseline development in accordance with MIL-STD-973, and should be documented in the prime and critical item (Type B) specifications and reviewed at the System Functional Review (SFR).

A5.4.2.3.1.10. Update/refine system security certification and accreditation requirements.

A5.4.2.3.1.11. Determine system security certification and accreditation agencies.

A5.4.2.3.1.12. System security engineering risk analysis, computer security risk analysis and studies should be conducted and integrated into the systems engineering documentation for Milestone C Review.

A5.4.2.3.1.13. If determined during Pre-Systems Acquisition that a System Concept of Operations (CONOPS) is required, the CONOPS should be updated to provide solutions to system's security engineering requirements.

A5.4.2.3.2. Functional analysis/allocation. The Government and contractor should both directly support the systems engineering (SE) activities in preparation for the Milestone C Decision Authority Review and Phase approval:

A5.4.2.3.2.1. Request for Proposal (RFP) - security requirements for the contractor.

A5.4.2.3.2.2. Statement of Objective (SOO).

A5.4.2.3.2.3. Contract Data Requirements List (CDRL).

A5.4.2.3.2.4. DD Form 254, **Contract Security Classification Specification**.

A5.4.2.3.2.5. Applicable Data Item Descriptions (DID).

A5.4.2.3.2.6. Source Selection Planning.

A5.4.2.3.2.7. Planning Instruments.

A5.4.2.3.2.8. System Requirements Review (SRR) - Review results of Phase A system security engineering activities.

A5.4.2.3.2.8.1. Special Access Security Plans.

A5.4.2.3.2.8.2. Computer Security Risk Analysis.

A5.4.2.3.2.8.3. Communication Security (COMSEC) Equipment Plans.

A5.4.2.3.2.8.4. Security Classification Guide.

A5.4.2.3.2.8.5. PPP.

A5.4.2.3.2.8.6. Physical Security System Concepts.

A5.4.2.3.2.9. Other security activities.

A5.4.2.3.2.9.1. Review of security activities and products by System Security Working Group (SSWG).

A5.4.2.3.2.9.2. Environmental issues addressed.

A5.4.2.3.2.9.3. TEMPEST requirements determined and reviewed by a Certified TEMPEST Technical Authority (CTTA).

A5.4.2.3.2.9.4. Develop system security requirements including risk assessments as part of the functional configuration baseline and documented in the system (Type A) specification.

A5.4.2.3.2.9.5. System Functional Review (SFR) - Participate in the SFR and review system security engineering activities in preparation for Milestone C review.

A5.4.2.4. Production & Deployment Phase.

A5.4.2.4.1. System Security Engineering requirements.

A5.4.2.4.1.1. Participate in Preliminary Design Review (PDR).

A5.4.2.4.1.2. Update/refine System Security Concept and System Security Management Plan.

A5.4.2.4.1.3. Finalize Product Security requirements and include in the solicitation for this phase.

A5.4.2.4.1.4. Update/refine system/subsystems interface specifications, system security engineering design, SVA, system architecture and threat analysis.

A5.4.2.4.1.5. Preliminary planning should begin to interface system security accreditation requirements to the Security Test and Evaluation (ST&E) and Operational Test and Evaluation (OT&E) Programs.

A5.4.2.4.1.6. A comprehensive ST&E Program should be developed (see [A5.4.2.5.1.](#)) and incorporated into the SE Test and Evaluation Master Plan (TEMP).

A5.4.2.4.1.7. ST&E requirements should be developed and included in the TEMP for Computer, Communications, TEMPEST, and Physical Security.

A5.4.2.4.1.8. Determine Designated Approving Authority (DAA) and Risk Approval Authority (RAA) for test activities. The ST&E results should form the basis for the DAA/RAA approval and subsequent system security accreditation.

A5.4.2.4.1.9. System security design characteristics should form part of the product configuration baseline in accordance with MIL-STD-973 and should be documented in the product (Type C) specifications. The test results (qualification tests and DT&E) should be reviewed to ascertain achievement of the desired system allocation and functional security requirement.

A5.4.2.4.1.10. System security engineering managers should participate in the functional configuration audit (FCA) when the product configuration is approved as having met contractual physical and functional requirements.

A5.4.2.4.1.11. Participate in Critical Design Review (CDR).

A5.4.2.4.1.12. Update/refine System Security Engineering requirements for Phase II in preparation for the Milestone III Review.

A5.4.2.4.2. System Design. System Design involves analyzing each security discipline to include physical and information systems protection requirements for the system's critical characteristics and capabilities. The portions of the system design that must be developed into the system to minimize and eliminate compromising the system or its technologies include:

A5.4.2.4.2.1. Classified Hardware. The objective is to design classified hardware by developing system security engineering through the identification of security discipline requirements throughout the system's engineering process. For additional information on computer security see AFI 33-202, *Computer Security*, and AFSSM 5010, *Computer Security in the Acquisition Life Cycle* (scheduled to be redesigned as AFMAN 33-226).

A5.4.2.4.2.1.1. Storage and handling requirements. System security engineering design requirements should be identified to minimize the numbers and sizes of classified equipment items. Facilities should be designed to provide a secure storage area for equipment items not installed on the system. Technical design features should assure integrity, availability, and confidentiality of equipment during transportation, storage, maintenance, and when installed in the system.

A5.4.2.4.2.1.2. Classified emanations. The system should be designed to avoid outside detection of classified intra and inter system data emanations. The individual items of equipment that are involved in this data flow should be TEMPEST designed to meet the requirements of AFI 33-203.

A5.4.2.5. Production & Deployment Phase. Systems and facilities should be formally tested, evaluated, and certified as to the effectiveness of the system's designed INFOSEC and physical security. Security system training plans should be prepared and implemented. The approved security baseline should be controlled by security participation in the Configuration Management (CM) Program. Operational system security engineering support activities should be initiated. The system security operations and support activities should directly support the companion SE activities performed in preparation for Milestone IV Decision Authority Review and subsequent phase approval. Deployment of a system should address environmental issues. Operational system security engineering support should be initiated in the Operations & Support Phase. Security program

status and results should continue to be presented to the government at required Program Reviews throughout sustainment and until demilitarization.

A5.4.2.5.1. Security Test and Evaluation (ST&E). System security engineering features should be verified through ST&E. The contractor should establish an ST&E Program that is fully integrated into the Program System's Test and Evaluation activities. System security engineering test activities should be coordinated and integrated to maintain program cost and schedule requirements. SSE should participate during scheduled DT&E/OT&E activities. Physical, communications, and computer security systems should be assessed for verification of requirements. A Security Test and Evaluation Plan and a Security Test and Evaluation Report should be developed and documented which correlates system requirements, assessment methods (analysis, inspection, demonstration and test), and deficiencies noted.

A5.4.2.5.2. Systems Test, Evaluation and Accreditation Process. Systems and facilities should be formally tested, evaluated, and certified as to the effectiveness of the system's designed INFOSEC and physical security. The accreditation process should use a common risk management methodology. The government program office should identify the Risk Acceptance Authority (RAA) to all participating contractors. The System Security Management Plan should define that methodology and the interfaces with the RAA. Where possible, a common RAA should be identified for the system, normally within the Operating Command that developed the Operational Requirements Document. Security Test and Evaluation plans, tests and reports should be used to support separate approval authorities when a single security risk manager cannot be designated. System changes should be controlled by the CM process and approved by the RAA/DAA for major system changes, or during a recertification/reapproval process.

A5.4.2.6. Operations & Support Phase. Continued system security engineering support should be provided to the operability, maintainability and reliability of the deployed system. System security engineering documentation, plans and analyses for sustainment should be updated, as required for system modifications, upgrades or changes in threat. Cost, schedule, security, and performance supervision, program reviews, risk management, System Safety, System Security Working Group (SSWG) participation, and continuation of the system security recertification process should be continued throughout sustainment and until system demilitarization.

A5.5. Detailed Requirements.

A5.5.1. System security engineering requirements.

A5.5.1.1. SSE applications.

A5.5.1.1.1. Secure system capabilities. Secure system capabilities should be addressed by the essential elements of the systems engineering process (requirements analysis, functional analysis/allocation, synthesis and analysis & control) throughout the acquisition cycle of the system. Software development should be accomplished in accordance with the direction of ISO/IEC 12207 and DoD-STD-2168. The level of effort should be commensurate with the contractual objectives for the definition of system products, processes and verification.

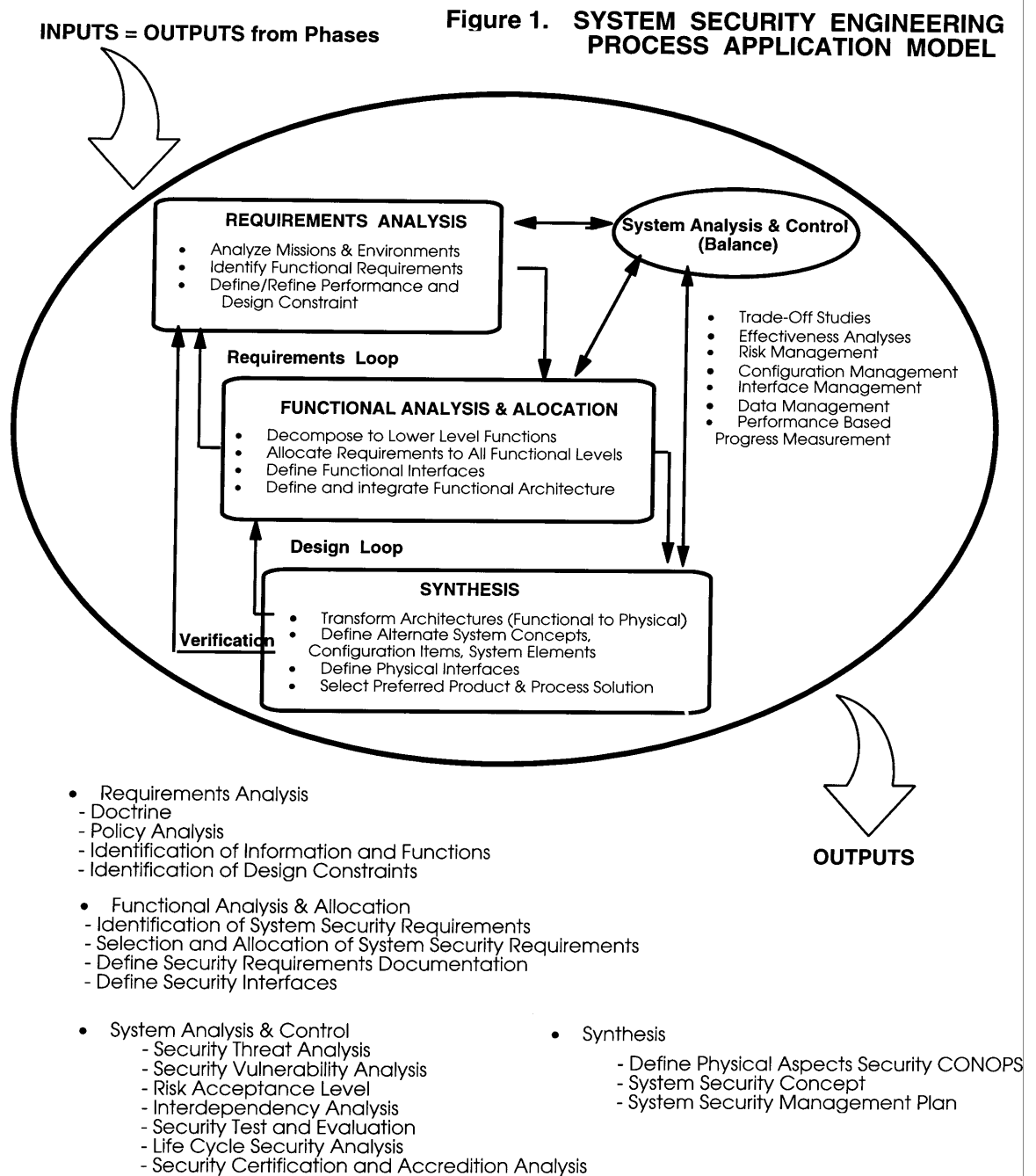
A5.5.1.1.2. Work Breakdown Structure (WBS). The "Systems Engineering/Program Management" element of the contract WBS, prepared per the guidance of MIL-HDBK-881, should be

extended to the level necessary to complete contractual SSE requirements, based on the Contract WBS.

A5.5.1.1.3. Secure system requirements. Assessment and review of progress, traceability of technical inputs and changes, data integration, configuration management and risk management, should be integrated into the secure system requirements.

A5.5.1.1.4. Logistics support. Provide SSE inputs to the Logistics Support Plan or an Appendix to the overall system logistics support plan. Identify for incorporation into the overall system logistics support plan the management objectives and procedures for accommodating logistics requirements associated with system security engineering designed into systems and subsystems.

A5.5.1.2. System security engineering process. Figure 1 depicts the relationship of SSE processes integrated with the systems engineering processes.



A5.5.1.2.1. Requirements analysis.

A5.5.1.2.1.1. System description. The system description should be documented to provide a data base for system sensitivity and criticality definition, and the SSE effort.

A5.5.1.2.1.2. Audit trail. An audit trail should be developed which provides traceability from requirements through system security engineering solutions, including associated costs, design and risk acceptance decisions. This audit trail should be documented in the Requirements Correlation Matrix (RCM).

A5.5.1.2.1.3. Security Threat Analysis (STA). The government System Threat Analysis Reports (STAR) should be reviewed to assure that both threats to intelligence collection and system denial in the system's proposed operational environment are addressed in the STA. The STA should correlate potential adversary/threat characteristics, postulated capabilities, and plausible political, economic and hostile adversary incentives during peace and increased international or domestic tension.

A5.5.1.2.1.4. System Vulnerability Assessment (SVA). Based on the STA, an SVA should be conducted using the system's operational environment and configuration requirements. All system elements should be addressed to include embedded computer and communications systems. Threat capabilities and characteristics should be compared to system components (hardware, software, computers, facilities, communications), operational procedures, logistics concepts, and support equipment. The sensitivity or criticality levels of system components, procedures and support elements should be identified and characterized, based on their value to the adversary threat.

A5.5.1.2.2. System Security Concept (SSC). Using results from the SVA, a SSC should be developed. Factors such as the system's critical characteristics and sensitivity levels to mission capability should be correlated with national security information categories, intelligence indicators, system operating modes, essential communication nodes, physical security criteria, and INFOSEC criteria (such as trusted computer system evaluation criteria, TEMPEST, etc) considerations in developing the SSC. The SSC requirements should be traceable to the system's specific security vulnerabilities and should identify those that are mitigated and those that require a RAA decision. The most beneficial risk acceptance level, in consideration for mission capability requirements, should be recommended. Manpower requirements to support the SSC should be identified.

A5.5.1.2.2.1. Configuration item documentation. Performance-based, multi-disciplined, functional system security engineering requirements documents and specifications should be generated, and documented in the related systems engineering configuration item documents.

A5.5.1.2.2.2. Security Trade Off Analysis. A Security Trade Off Analysis (STOA) should be conducted using the SSC. System security applications for INFOSEC (such as COMPUSEC, COMSEC, TEMPEST, etc.) and physical security and their individual initial and recurring costs for both manpower and equipment should be identified. A graduated trade off methodology should be used portraying most effective to least effective by total cost.

A5.5.1.2.2.3. Level functions. Successively lower level functions required to satisfy higher level functional requirements should be defined.

A5.5.1.2.3. Synthesis/integration.

A5.5.1.2.3.1. Security features of the functional system elements. The security features of the functional system elements should be defined. The security features should completely satisfy the requirements of the System Security Concept, system operational performance characteristics, and system descriptions.

A5.5.1.2.3.2. Security system and security requirements interfaces. The security system and security requirements interfaces with other internal system components or external system connections should be defined. Security requirement conflicts and proposed corrective measures should be identified. System Vulnerability Analysis and System Security Concept documentation should be updated.

A5.5.1.2.3.3. Standardization and interoperability requirements for disclosure to Foreign Governments. Modular product designs should minimize the degradation associated with classified portions of the system's functions that are restricted from disclosure to foreign governments.

A5.5.1.2.3.4. System Security Engineering environmental issues. Systems engineering should include system security engineering requirements that address environmental issues. The Systems Engineering Management Plan (SEMP) should be used to ensure the contractor is aware of the Government's requirements to minimize potential environmental impacts. The systems engineering process should account for the product throughout its life cycle (concept exploration/definition through operation support and the final disposal). Environmental conditions should address hazardous materials/hazardous waste. A priority of the systems engineering processes should be used to minimize the need for pollution control by designing out the use/creation of hazardous substances. The order of preference for environmental issues is prevention, conservation, compliance, and restoration.

A5.5.1.2.4. Design. System security engineering requirements and security systems should be translated into system hardware, software, facility, communications and computer design specifications and documentation, and validated during design reviews. Impacts of engineering changes on the documented SVA and SSC should be assessed. The security system design should be documented for risk acceptance authorities.

A5.5.1.2.5. Risk assessment/acceptance. Use the STA, SVA, SSC, STOA and ST&E to determine the level of security risk. Specific corrective actions, compensatory measures or recommendations for risk acceptance decision by the RAA should be identified in the ST&E report. If appropriate, based upon the seriousness of any residual risks, such information should be provided to the Milestone Decision Authority as "exit criteria."

A5.5.2. Security organization. An acquisition security management function should be established as an element of the Government program management staff to provide multi-role security support to contract program management in supporting the SSE management objectives. Security discipline activities within this office should be integrated to provide continuity of effort, consistency, and application of inter-related security discipline analyses to both system and program security planning, requirements definition, design, test, and sustainment activities.

A5.5.3. System Security Working Groups (SSWG). A SSWG should be established IAW AFI 63-1701, Chapter 3. The implementation of the SSWG should be tailored to the specific requirements of each program. The purpose of the SSWG should be to review and integrate all SSE activities,

resolve security issues and review recommended risk management assessments. The use of concurrent engineering teams should be encouraged to assure early and continuous review of systems development activities for security risk and configuration management control, full understanding of security requirements, solutions and a complete integration of SSE activities to other engineering elements.

A5.5.4. Configuration management (CM). System security engineering configuration control should be required to protect the approved security baseline from unauthorized manipulation and undocumented changes. System security engineering configuration should be achieved by the Security Compliance/Accreditation programs and through security participation within the System CM Program. All secure systems and facilities should be protected from unauthorized modifications at all times. All proposed changes should be authorized and fully documented by the formal CM process. Direct SSE representation within the CM process should ensure continuity of the approved security baseline.

A5.5.5. SSE data requirements. The National Disclosure Policy for U.S. technical data should be used to determine classification and category of appropriate data.

A5.6. Notes. (This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

A5.6.1. Intended use. This process tool is intended for use by government agencies and defense contractors for development of system security engineering criteria and applications as required by the defense acquisition process. It establishes the guidance necessary to implement and manage SSE programs and products.

A5.6.2. Acquisition requirements. Acquisition documents must specify the following:

A5.6.2.1. Title, number, and date of the specification.

A5.6.2.2. Issue of DoDISS to be cited in the solicitation, and if required, the specific issue of individual documents referenced.

A5.6.3. Consideration of data requirements. Data requirements should be considered when this process tool is applied on contract. The applicable DID should be reviewed with each specific program acquisition to ensure that only essential data are requested/provided and that the DID is tailored to reflect the specific requirements of each acquisition.

Appendix A5A

GLOSSARY

Accreditation—A formal declaration by the Designated Approving Authority (DAA) that a system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an Automated Information System (AIS) and is based on the certification process as well as other management considerations. An accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Adversary—An individual, group, organization, or government that must be denied access to essential information, technologies, systems or subsystems. Also anyone that presents the possibility of causing any intentional circumstance or event with the potential to cause harm to a system.

Automated Information System (AIS)—An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Certification—The comprehensive evaluation of the technical and nontechnical security features of a system and other safeguards, made in support of the accreditation process, which establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Compromise—Disclosure of information or data to unauthorized person(s), or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss may have occurred.

Compromising Emanations—Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment. (See TEMPEST)

Configuration Item (CI)—An aggregation of hardware, firmware, or computer software or any of their discrete portions, which satisfies an end use function and is designated by the Government for separate configuration management. Configuration items may vary widely in complexity, size, and type, from an aircraft, electronic, or ship system to a test meter or round of ammunition. Any item required for logistic support and designated for separate procurement is a configuration item.

Critical Program Information (CPI)—That information about the program, technologies, and/or systems that if compromised would degrade combat effectiveness or shorten the expected effective life of the

system. Unauthorized access to this information or systems could allow someone to kill, counter, or clone the system before or near scheduled deployment, forcing a major design change to maintain the same level of effectiveness and capability.

Evaluation—A subjective technical judgment made by a qualified analyst as to the value or worth of a particular implementation based upon the analyst past experience and subject matter knowledge.

Information System—Any telecommunication and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

Information System Security (ISS)—The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Maintainability—A measure of the time or maintenance resources needed to keep an item operating or to restore it to operational status (or serviceable status). Maintainability may be expressed as the time to do maintenance (for example, maintenance downtime per sortie), as a usage rate (for example, maintenance work hours per flying hour), as the staff required (for example, maintenance personnel per operational unit), or as the time to restore a system to operational status (for example, mean downtime).

Milestone Decision Authority (MDA)—The individual designated in accordance with criteria established by DoD to approve entry of an acquisition program into the next phase of the acquisition process.

Operational Requirements Document (ORD)—A user command prepared document that is initially prepared during Phase 0 and describes preliminary system-specific characteristics, capabilities, and other related operational variables. ORDs are updated and expanded for each milestone. The Chief of Staff of the Air Force approves all Air Force and Air Force lead ORDs.

Operational Test and Evaluation (OT&E)—Test and evaluation, initial operational test and evaluation, and follow-on OT&E conducted in a realistic and operational environment as possible to estimate the prospective system's operational effectiveness and suitability. OT&E provides information on organization, personnel requirements, doctrine, and tactics, and provides data to support material in operating instructions, publications, and handbooks.

Program Information—Information that includes programmatic data/information and weapons system, subsystem, or component information.

Program Protection—The safeguarding of critical systems and subsystems anywhere in the acquisition process to include the technologies being developed, the support systems (i.e., test and simulation equipment) and research data with military applications. This protection activity involves integrating all security disciplines, counterintelligence, and other defensive methods to protect the CPI against unauthorized disclosure or access.

Program Protection Plan (PPP)—A comprehensive protection and technology control management tool established for each defense acquisition program to identify and protect classified, unclassified/sensitive information and critical systems and subsystems.

Requirements Correlation Matrix (RCM)—That portion of the ORD that tracks and displays essential user needs and requirements over the program life cycle. RCMs are mandatory for Air Force and Air Force lead-developed ORDs.

Risk Acceptance Authority—A government official, usually from the agency which will operate the system being acquired, who is designated to make risk acceptance decisions for all system security inadequacies.

Risk Acceptance Level—A Risk Acceptance Authority's determination of the level of protection deemed adequate. This is a risk management decision, not risk avoidance, and is usually made by an official from the operating activity that will use the system being acquired.

Security Criteria—The performance requirements that provide a maximum degree of risk mitigation at the lowest cost.

Security System—The aggregate of all mechanical and electronic hardware, software, and procedural security countermeasures in a system that minimizes risks of denial, compromise or alteration.

Security Test and Evaluation (ST&E) Report—The formal documentation of all system security engineering testing and all of the security features for the computer, communications, TEMPEST and physical security measures designed into the system. The report includes testing methodology, results, risk assessments and acceptance recommendations, and any suggested exit criteria for the MDA to use in determining whether or not to proceed into the next acquisition phase.

Security Threat Analysis (STA)—The formal documentation of all system security threats.

Security Trade Off Analysis (STOA)—The formal documentation of all trade-off considerations for computer, communications, TEMPEST and physical system security applications.

Subsystem—An element of a system that, in itself, may constitute a system.

System—An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

System Security Concept (SSC)—The formal documentation of conceptual measures to be taken for computer, communications, TEMPEST, and physical system security countermeasures for the acquired system's critical characteristics and sensitivity levels to achieve successful mission capability.

System Security Engineering (SSE)—A functional area of systems engineering that applies scientific and engineering principles to identify system security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of system to security threats.

System Security Engineering Management—An element of program management that ensures system security tasks are completed. These tasks include developing security requirements and objectives; planning, organizing, identifying, and controlling the efforts that help achieve security and survivability of the system during its life cycle, and interfacing with other program elements to ensure all security disciplines (industrial, information, physical and personnel in addition to the specialized security elements of COM-PUSEC, OPSEC, COMSEC and nuclear security) are effectively integrated into the total system engineering effort.

System Threat Assessment Report (STAR)—The authoritative assessment, tailored for and focused on, a particular U.S. major defense system. It describes the battlefield threat to be countered and the projected threat environment.

System Vulnerability Analysis (SVA)—The formal documentation of all system security vulnerabilities that would be experienced by the system's configuration in its operational environment.

Technology—The information and know-how that can be used to design, produce, manufacture, utilize, or reconstruct goods.

TEMPEST—Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (See compromising emanations.)

Threat—The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system or equipment mission effectiveness.

Threat Risk—The level of vulnerability associated with an adversary's capability, plus the probability of an actual adversary's effort.

Trusted Computing Base (TCB)—The totality of protection mechanisms within a computer system—including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (such as a user's clearance) related to the security policy.

Vulnerability—The susceptibility of systems or subsystems to the threat in a given environment that could result in system susceptibility to modification/tampering, compromise, denial of service or destruction.

Appendix A5B**ACRONYMS**

AIS—Automated Information System
ASR—Alternate System Review
CDR—Critical Design Review
CM—Configuration Management
COMSEC—Communications Security
COMPUSEC—Computer Security
CPI—Critical Program Information
CTTA—Certified TEMPEST Technical Authority
DAA—Designated Approving Authority
DID—Data Item Description
DT&E—Developmental Test and Evaluation
FAR—Federal Acquisition Regulation
FCA—Functional Configuration Audit
FR—Functional Review
INFOSEC—Information Security
ISS—Information System Security
ORD—Operational Requirement Document
OT&E—Operational Test and Evaluation
PDR—Preliminary Design Review
PPP—Program Protection Plan
RAA—Risk Acceptance Authority
RCM—Requirements Correlation Matrix
RFP—Request for Proposal
SE—Systems Engineering
SOO—Statement of Objective
SFR—System Functional Review
SRR—System Requirements Review

SSC—System Security Concept

SSE—System Security Engineering

SSWG—System Security Working Group

STA—Security Threat Analysis

STAR—System Threat Assessment Report

ST&E—Security Test and Evaluation

STOA—Security Trade Off Analysis

SVA—Security Vulnerability Analysis

TEMP—Test and Evaluation Master Plan

TEMPEST—Technical Electro-Magnetic Pulse Emanation Suppression Techniques

WBS—Work Breakdown Structure